EU General Data Protection Regulation Sanctions in Theory and in Practice

W. Gregory Voss, Hugues Bouthinon-Dumas

Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 37 | Issue 1 Article 2

1-1-2021

EU GENERAL DATA PROTECTION REGULATION SANCTIONS IN THEORY AND IN PRACTICE

Voss, W. Gregory

Bouthinon-Dumas, Hugues

EU GENERAL DATA PROTECTION REGULATION SANCTIONS IN THEORY AND IN PRACTICE

By W. Gregory Voss[i] & Hugues Bouthinon-Dumas[ii]

Prior to the application of the EU General Data Protection Regulation (GDPR), one result of the low maximum corporate fines for violations under the preceding data protection legislation was, arguably, a lack of compliance by U.S. Tech Giants and other companies. At least on paper, this changed under the GDPR. This study approaches the issue of GDPR sanctions, not through the lens of a catastrophe waiting to happen, but instead though a development first of the theoretical grounds for sanctions, prior to a view of the practical side of them. In doing so, it is somewhat unique and adds to the GDPR literature. Furthermore, it engages the legal strategy and compliance literature to bring its results home to inform companies as to the risks involved and to provide strategic recommendations both for companies and for regulators.

Among the several sub-goals of sanctions, this study determines that the most relevant for an analysis of GDPR sanctions—which are administrative, regulatory and financial sanctions, in large part—is the deterrence function, beyond the symbolic functions. This demands effective and substantial administrative fines. While these are not the only sanctions available under the GDPR—this study also sets out a range of possible sanctions, such as judicial compensation and orders to halt data processing—they are perhaps the most characteristic of data protection enforcement. However, through what is referred to as the one-stop-shop mechanism, the Irish DPA is the lead authority for most of the U.S. Tech Giants, and it has failed to act against them up to now, resulting in a potential lack of deterrence. This study argues that, on the one hand, companies should embrace compliance, and on the other hand, truly dissuasive administrative fines must be issued by supervisory authorities when they are justified, in order for the sanctions to have their necessary deterrence effect.

---

[i] Associate Professor, TBS Business School, Toulouse, France. This co-author may be contacted at g.voss@tbs-education.fr.

[ii] Associate Professor of Law, ESSEC Business School, Paris, France. This co-author may be contacted at bouthinondumas@essec.edu.

CONTENTS

INTRODUCTION

The European Union's General Data Protection Regulation (GDPR),[1] which has applied since May 25, 2018,[2] has extraterritorial effect,[3] much as its predecessor legislation—the EU Data Protection Directive[4]—did, but more so. However, such extraterritorial effect is—this study argues—not of much use without effective incentive for compliance and means of enforcement. In November 2015, a little more than one month before political agreement was reached on EU data protection law reform,[5] and more than five months before its adoption in the form of the GDPR,[6] then-French State Secretary for Digital Matters Axelle Lemaire estimated that the power to sanction of the French data protection authority–the CNIL (*Commission Nationale de l'Informatique et des Libertés* [National Commission for Computing and Liberties])–was "peanuts" compared to the economic reality of Internet giants, especially U.S. companies that dominate the market.[7]

---

[1] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [hereinafter GDPR].

[2] *Id*. art. 99(2).

[3] For a brief discussion of this extraterritorial effect, *see infra* Section A of the Introduction.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data personal data and on the free Movement of such data, 1995 O.J. (L 281) 31, 31 [hereinafter EU DP Directive].

[5] Political agreement was reached on EU data protection reform on December 15, 2015. *See* European Commission Press Release IP/15/6321, *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market* (Dec. 15, 2015). https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321. Note that the term "data protection," is used within the European Union.

[6] Various dates have been used for the adoption date of the GDPR. Certain authors use the date it was approved by the Council of the European Union. Some use the date that the GDPR was approved by the European Parliament; others, the date of its publication in the Official Journal of European Union, or twenty days thereafter, when it entered into force. The GDPR was actually signed and dated on April 27, 2016. GDPR, *supra* note 1 ("Done at Brussels, 27 April 2016").

[7] Fabienne Schmitt, *Le pouvoir de sanction de la CNIL, « c'est cacahouète »* [The CNIL's Sanctioning Power: "It's Peanuts"], LESECHOS.FR (Nov. 3, 2015), https://www.lesechos.fr/03/11/2015/LesEchos/22058-101-ECH_le-

At the time the maximum administrative sanction that the CNIL was able to impose was €150,000,[8] or the then-equivalent of approximately $165,000.[9] This was a sum that then-EU Justice Commissioner Viviane Reding described as "pocket money," when in 2014 the CNIL issued a fine against Google in that amount.[10]

However, since May 25, 2018, the date the GDPR first applied,[11] EU Member State data protection supervisory authorities such as the CNIL can issue administrative sanctions for the most severe data protection violations by companies in the amount of the greater of €20 million or 4% of worldwide annual turnover for the prior year.[12] At least on paper, it's not peanuts anymore! Much attention has been paid to this increase in potential EU sanctions for data protection violations.[13] This is comprehensible given the importance of data in

---

pouvoir-de-sanction-de-la-cnil----c-est-cacahouete--.htm?texte=LESECHOS:%20Le%20pouvoir%20de%20sanction%20de%20la%20CNIL,%20«%20c'est%20cacahouète%20».

[8] *See* Hazel Grant & Hannah Crowther, *How Effective Are Fines in Enforcing Privacy?*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 287, 301 (David Wright & Paul De Hert, eds., 2016).

[9] *Currency Converter*, OANDA, https://www.oanda.com/lang/fr/currency/converter/ (calculated using historical currency exchange figures for Nov. 3, 2015).

[10] *See* European Commission Press Release, *Speech: The EU Data Protection Reform: Helping Businesses Thrive in the Digital Economy* (Jan. 14, 2014), http://europa.eu/rapid/press-release_SPEECH-14-37_en.htm ("Taking Google's 2012 performance figures, the fine in France represents 0.0003% of its global turnover. Pocket money."). One journalist referred to a 2017 CNIL fine against Facebook in the same amount as a "slap on the wrist." *See also* Mark Scott, *Facebook Gets Slap on the Wrist from 2 European Privacy Regulators*, N.Y. TIMES (May 16, 2017), https://nyti.ms/2rlzS4O.

[11] GDPR, *supra* note 1, art. 99(2).

[12] *Id.* art. 83(5).

[13] *See*, *e.g.*, ONNO JANSSEN ET AL., THE PRICE OF DATA SECURITY: A GUIDE TO THE INSURABILITY OF GDPR FINES ACROSS EUROPE 3 (3rd ed., 2020) ("The scale of these fines has understandably generated concern in boardrooms. GDPR has replaced a regime under which fines for a data breach were limited and enforcement actions infrequent. The regulatory environment across European Member States is undoubtedly shifting and regulators now have greater powers of enforcement, and significant GDPR fines are expected to be imposed where organisations are subject to investigations."), https://www.dlapiper.com/en/uk/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/. *See also* Omer Tene, *With Hefty GDPR Fines, a New Industry Emerges*, IAPP (July 12,

today's economy—described variously as the new gold or the new oil[14] —and due to the extraterritorial reach of the GDPR. This study looks at these sanctions and other remedies under the GDPR both from theoretical and practical perspectives. The essential research question posited by this study is, *does the reality of supervisory authority action support the theoretical goals for GDPR sanctions, and what strategic recommendations for both firms and supervisory authorities result?*

This introduction continues with an initial brief explanation of the GDPR (Section A), followed by a discussion of the U.S. Tech Giants (Section B)—companies whose business model may be strongly impacted by the GDPR due to their use of personal data,[15] and ending with an introduction on data protection sanctions (Section C).

A. The EU General Data Protection Regulation (GDPR)

The GDPR is the European Union's omnibus data protection legislation,[16] taking the form of an EU regulation, which means that it

---

2019), https://iapp.org/news/a/with-hefty-gdpr-fines-a-new-industry-emerges/ (discussing the new privacy tech industry, the author comments about the effect of GDPR fines: "With mega fines come heightened responsibilities for companies, directors and officers.").

[14] *See*, *e.g.*, W. Gregory Voss, *Internet, New Technologies, and Value: Taking Share of Economic Surveillance*, 2017 U. ILL. J.L. TECH. & POL'Y 469, 471 (2017).

[15] *See, e.g.*, Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L & TECH. 1, [1]–[5] (2018); *see also* David Meyer, *Europe's Privacy Laws are Tough. Meet the Woman Who Could Make Them Costly for Facebook and Google*, FORTUNE (Oct. 28, 2019, 3:30), https://fortune.com/2019/10/28/gdpr-europe-helen-dixon-ireland-privacy-laws-facebook-google/ ("If the U.S. firms lose in major cases, Dixon could order them to pay fines as high as 4% of global annual revenue; a negative ruling could also expose them to even more expensive civil suits. More importantly, they may face new limits on how they acquire, share, and use personal data—the lifeblood of today's ad-driven tech economy.").

[16] Omnibus (or comprehensive) data protection legislation contrasts with the U.S. sectoral/self-regulatory model. *See* W. Gregory Voss, *Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation*, 50 REVUE JURIDIQUE THÉMIS 783, 789 (2018). Note that the GDPR also applies in the European Economic Area (EEA) Agreement countries of Iceland, Norway and Lichtenstein. In this sense, s*ee also* Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], 2018 O.J. (L 183) 23. Nonetheless, this study will continue to refer to the European Union in its discussion of the GDPR.

is directly applicable throughout the European Union.[17] The GDPR has a dual objective—to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"[18] and to guarantee the "free movement of personal data" within the European Union.[19] The GDPR recognizes that, thanks to new technologies, private companies (such as the U.S. Tech Giants), are able "to make use of personal data on an unprecedented scale in order to pursue their activities."[20] As a result, there is a need to make operators more responsible and to have strong enforcement by the regulatory authorities, with a view to creating trust in the digital economy.[21] The GDPR stipulates that in order for personal data—a very broad concept in the European Union drafted to include a range of information that can be tied to an identified or identifiable natural

[17] *See* Consolidated Version of the Treaty on the Functioning of the European Union, art. 288, 2012 O.J. (C 326) 1, 171–72 [hereinafter TFEU]. *See also* Irina Alexe, *The Sanctioning Regime Provided by Regulation (EU) 2016/679 on the Protection of Personal Data*, 2017 INT'L LAW REVIEW 60, 61 (2018).
[18] GDPR, *supra* note 1, art. 1(2). This right to personal data protection is enshrined in the TFEU. *See* TFEU, *supra* note 17, art. 16. It is also contained in the Charter of Fundamental Rights of the European Union. *See* Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, 397. Article 8(1) of the Charter of Fundamental Rights of the European Union provides "Everyone has the right to the protection of personal data concerning him or her." For a discussion of the modification of the legal status of the Charter of Fundamental Rights of the European Union to make it legally binding, and for the incorporation of the right to personal data protection into the TFEU, *see* GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 231–234 (2014).
[19] GDPR, *supra* note 1, art. 1(3). This is part of what Lynskey refers to as part of the "economic underpinning" of the legislation. *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 8 (2015). Lynskey also discusses the legislative goal of market harmonization. *Id*. at 66-67 ("The increased emphasis on the effectiveness of fundamental rights in the Commission's proposal for a Regulation did not detract attention from its emphasis on market harmonization … the substantive provisions of the Commission's initial proposal also evidenced its ambition to create a uniform regulatory environment for data processing in the EU.").
[20] GDPR, *supra* note 1, Recital 6.
[21] *Id*. Recital 7.

person (data subject)[22]—to be processed (another broad term),[23] there must be a legal basis for such processing, such as consent, when the GDPR applies.[24] Moreover, a large range of rights must be furnished to data subjects,[25] and data information principles (similar to fair information principles) apply,[26] including the requirement that measures must be taken to ensure the security of the personal data.[27] The GDPR operates when its provisions regarding material and territorial scope are met,[28] among which, new extraterritorial coverage

---

[22] "Personal data" are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 1, art. 4(1). For a discussion of the broadness of this term and its meaning, *see* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 313–24 (2019). For an earlier development of this issue, prior to the finalization of the GDPR, *see* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 877 (2014).

[23] "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, *supra* note 1, art. 4(2).

[24] Consent is one of six legal bases for the processing of personal data. The others are where the processing is necessary for: the performance of a contract to which the data subject is a party, compliance of a legal obligation of the controller, the protection of the data subject's (or another individual's) vital interests, the performance of a public interest task or one under public authority, or the controller's legitimate interest. However, this last basis may be overridden by the data subject's fundamental rights. *Id*. art. 6(1).

[25] These include information requirements with respect to the processing. *Id*. arts. 13–14. A right of access to his or her data is provided, as well. *Id*. art. 15. A right to rectification applies, too. *Id*. art. 16. Furthermore, there is a new right to erasure ("right to be forgotten"). GDPR, *supra* note 1, art. 17. A right to obtain restrictions of processing is furnished in certain circumstances. *Id*. art. 18. In addition to other rights, there is a new right to data portability. *Id*. art. 20. For other rights (right to object and right not to be subjected to automated individual decision-making), *see id.* arts. 21–22.

[26] *Id*. art. 5.

[27] GDPR, *supra* note 1, art. 5(1)(f).

[28] *Id*. arts. 2–3.

where data of data subjects in the European Union are being processed in connection with the offer of goods or services (whether for pay or in exchange for the personal data, without payment) or where the behavior of data subjects in the European Union is being monitored, when such behavior occurs within the European Union.[29] In such cases, the companies collecting and processing the data do not need to have an establishment in the European Union in order to be required to comply with the GDPR, but they may be required to appoint a representative in the European Union.[30]

B. The U.S. Tech Giants

As measured almost three and one-half years after Axelle Lemaire spoke, and ten months after the GDPR became applicable, five of the six largest U.S. firms by market value were in the sector of information technology and Internet (including e-commerce and social media): (in order) Microsoft, Apple, Amazon, Alphabet (Google), and Facebook.[31] One journalist has referred to these companies, which each amass tens of billions of dollars in revenue annually, as the "Frightful Five," and has remarked upon the domination of these firms, and their recent loss of goodwill both among the public and U.S. regulatory and legal infrastructure, as such firms have moved from "disrupters" to "incumbents."[32] These same firms have been referred to by Europeans as the "GAFAM" (for Google, Apple, Facebook, Amazon, and Microsoft),[33] and such firms have similarly lost goodwill, especially since the revelation of the N.S.A. PRISM mass surveillance

---

[29] The new provision reads:

> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behavior as far as their behavior takes place within the Union. *Id*. art. 3(2).

[30] *Id*. art. 27.

[31] The ranking is as of March 29, 2019. The other firm making up the six largest market valuations was Berkshire Hathaway, at fourth place, ahead of Amazon. *See Fortune 500,* FORTUNE 2019, https://fortune.com/fortune500/2019/search/.

[32] Farhad Manjoo, *Tech Giants Seem Invincible. That Worries Lawmakers.*, N.Y. TIMES (Jan. 4, 2017), https://nyti.ms/2jD5mCK.

[33] For a discussion of this, *see* Voss, *supra* note 14, at 474 n.28.

program[34] involving the participation of all but one of them.[35] Another term used has been "Big Tech."[36] For ease of reference and to retain the tie to their nation of origin, this study retains the use of the term "the U.S. Tech Giants,"[37] keeping in mind that this grouping is established merely as a shorthand way of discussing the largest U.S. technology companies, and that there are many distinctions between the companies that make up such grouping.[38] Much of what is said about the U.S. Tech Giants also applies to other U.S. companies mainly active on the Internet, such as Netflix, Airbnb, Tesla, and Uber, which have also been referred to as the "NATU."[39]

Certain of the U.S. Tech Giants have been the subject of prosecution or investigation in Europe for tax and competition law violations, areas of law often categorized as falling within the ambit of international economic law (IEL).[40] At the EU level, for instance, the

---

[34] *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://nyti.ms/2nJdWCF.

[35] *See* GLENN GREENWALD, NO PLACE TO HIDE 107–09 (2014). The lone exception was Amazon.

[36] For use of the term "big tech," *see, e.g.*, Sherrod Brown, *Privacy Isn't a Right You Can Click Away*, WIRED (June 29, 2020, 9:00 AM), https://www.wired.com/story/privacy-isnt-a-right-you-can-click-away/. *See also* Adam Satariano & Matina Stevis-Gridneff, *Big Tech's Toughest Opponent Says She's Just Getting Started*, N.Y. TIMES (Nov. 19, 2019), https://nyti.ms/2QA8ZtF (discussing EU competition law enforcement efforts against companies such as Apple, Uber, Amazon, Facebook and Google).

[37] For prior use of this term, *see, e.g.*, Ellen Huet & Alex Webb, *US Tech Giants Face Splintered Digital Future in EU*, SFGATE (June 28, 2016; updated, June 28, 2016 4:42 PM), https://www.sfgate.com/business/article/US-tech-giants-face-splintered-digital-future-in-8330585.php).

[38] *See e.g.*, Voss & Houser, *supra* note 22, at 332–38 (contrasting the legal strategy pathways of Facebook and Google, on the one hand, and Amazon, Microsoft and Apple, on the other hand).

[39] *See* Pierre Haski, *Après les Gafa, les nouveaux maîtres du monde sont les Natu* [*After the Gafa, the New Masters of the World are the Natu*], L'OBS AVEC RUE 89 (Jan. 26, 2017, 12:56 PM), https://www.nouvelobs.com/rue89/20150802.RUE3739/apres-les-gafa-les-nouveaux-maitres-du-monde-sont-les-natu.html.

[40] "Tax activity" and "corporate activity" that is the subject of bilateral or other international treaties, is considered to be part of international economic law (IEL). *See* JOHN H. JACKSON, SOVEREIGNTY, THE WTO, AND CHANGING FUNDAMENTALS OF INTERNATIONAL LAW 46 (2006). *See also* Steve Charnovitz, *What Is International Economic Law?*, 14 J. INT'L ECON. L. 3, 5–6 (2011) (including competition/antitrust and double taxation in the definition of international economic law, as legal norms "legislated (or alluded to) in the

European Commission concluded that Luxembourg tax rulings in favor of Amazon constituted illegal state aid in an amount of $295 million (€250 million) and must be recovered from Amazon by Luxembourg,[41] and likewise that two Irish tax rulings in favor of Apple constitute illegal state aid in an amount of up to €13 billion, which must be recovered from the company by Ireland.[42] However, the decision in the Irish tax rulings case was eventually annulled by the General Court of the European Union,[43] although such annulment is being appealed by the Commission,[44] and various EU member state efforts to recover taxes from certain U.S. Tech Giants have resulted in settlements.[45]

---

law of the World Trade Organization (WTO)." Charnovitz even includes legal norms regarding "the internet" as part of "international legal norms that are not part of the WTO," which fit within the definition of international economic law).

[41] *See* European Commission Press Release IP/17/3701, State Aid: Commission finds Luxembourg gave illegal tax benefits to Amazon worth around €250 million (Oct. 4, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3701. *See also* Robert-Jan Bartunek, *EU Orders Amazon to Repay $295 Million in Luxembourg Back Taxes*, REUTERS (Oct. 4, 2017, 2:37 AM), https://www.reuters.com/article/us-eu-amazon-taxavoidance/eu-orders-amazon-to-repay-295-million-in-luxembourg-back-taxes-idUSKCN1C913S.

[42] Commission Decision 2017/1283, on State Aid SA.38373 (2014/C) (ex 2014/NN) (ex 2014/CP) implemented by Ireland to Apple, 2017 O.J. (L 187) 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D1283&from=EN. In 2017, the European Commission referred Ireland to the Court of Justice of the European Union for failure to recover such amounts. *See also* Press Release, European Commission, State Aid: Commission refers Ireland to Court for failure to recover illegal tax benefits recover illegal tax benefits from Apple worth up to €13 Billion (Oct. 4, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3702.

[43] European Union Press Release 90/20, General Court of the European Union, The General Court of the European Union annuls the decision taken by the Commission regarding the Irish tax rulings in favour of Apple (July 15, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200090en.pdf.

[44] Foo Yun Chee, *EU's Vestager Appeals Court Veto of $15 Billion Apple Tax Order*, REUTERS (Sept. 25, 2020 11:52 AM), https://www.reuters.com/article/us-eu-apple-taxation-idUSKCN26G1DB.

[45] *See, e.g.*, Daniel Boffey & Jill Treanor, *Google £130m UK Back-Tax Deal Lambasted as 'Derisory' by Expert*, THE GUARDIAN (Jan. 23, 2016, 17:05), https://www.theguardian.com/technology/2016/jan/23/google-uk-back-tax-deal-lambasted-as-derisory (discussing £130 million settlement between Google and the UK); *See also* Reuters Staff, *Amazon to Pay 100 Million Euros*

France adopted a "GAFA" (or digital services) tax, aimed at ensuring that the U.S. Tech Giants pay a fair share of their French revenue to the French tax authorities,[46] and other European countries are considering similar measures.[47]

Furthermore, EU competition law sanctions have involved significant sums of money—in a 2013 report, prior to the application of the GDPR, EU competition law fines were shown to have an impact on U.S. international transactions accounts, while EU data protection fines were absent from the analysis.[48] EU competition law cases have resulted in fines of €561 million against Microsoft for not complying with anti-tying commitments in an antitrust case involving Internet

---

to Settle Italy Tax Dispute, REUTERS (Dec. 15, 2017, 5:03 AM), https://www.reuters.com/article/us-amazon-italy-tax/amazon-to-pay-100-million-euros-to-settle-italy-tax-dispute-idUSKBN1E91KM (reporting agreement between the Italian tax authority and Amazon to collect €100 million ($118 million) in back taxes for the period 2011–2015*); See also* Mark Scott, *Google Agrees to Pay Italy $334 Million in Back Taxes*, N.Y. TIMES (May 4, 2017), https://nyti.ms/2pL2Z3Z (detailing agreement between Italian authorities and Google to recover €306 million ($334 million) in back taxes for 2002–2015 and mentioning a similar 2015 agreement between Apple and Italy for €314 million in back taxes); Microsoft has also agreed to enter into an agreement with the French Ministry in charge of taxation for €350 million for corporate income tax for the period 2010–2012. *See* David Bensoussan, *Microsoft passe un accord avec le fisc français* [*Microsoft Makes an Agreement with the French Tax Authorities*], CHALLENGES (June 5, 2019, 18:58), https://www.challenges.fr/economie/microsoft-passe-un-accord-avec-le-fisc-francais_657176.

[46] *See* Liz Alderman, *France Moves to Tax Tech Giants, Stoking Fight with White House*, N.Y. TIMES (July 11, 2019), https://nyti.ms/2Lh1iXo. France has delayed collecting such tax—also referred to as a digital services tax—in order to allow time to negotiate a deal on the resulting dispute with the United States through the OECD. France had planned to collect such tax starting at the end of 2020. *See also* Mark Sweney, *UK and Europe Renew Calls for Global Digital Tax as US Quits Talks*, THE GUARDIAN (Jun. 18, 2020, 9:40), https://www.theguardian.com/media/2020/jun/18/uk-europe-global-digital-tax-us-quits-talks-tech.

[47] *See* Lilian V. Faulhaber, *Beware. Other Nations Will Follow France With Their Own Digital Tax.*, N.Y. TIMES (July 15, 2019), https://nyti.ms/2XKGsBC.

[48] *See* Christopher L. Bach, *Fines and Penalties in the U.S. International Transactions Accounts*, BEA 57 (July 2013), https://apps.bea.gov/scb/pdf/2013/07%20July/0713_fines_penalties_international_accounts.pdf.

Explorer and Windows OS software,[49] periodic penalties of €899 million against Microsoft in an antitrust case involving a refusal to provide interoperability information to vendors of work group server operating system products.[50] The European Commission has also fined Google €2.42 billion for abusing dominance as a search engine by giving illegal advantage to its own comparison shopping service,[51] and more recently €4.34 billion (or $5.1 billion[52]) for illegal actions related to the Android mobile operating system, which were aimed at strengthening Google's dominant position in internet search,[53] and €1.49 billion for abuse of its dominant position in online search advertisements through restrictive AdSense for Search contractual clauses requiring publishers using AdSense for Search to effectively reserve the most profitable spaces in their search results for Google advertisements, thereby disfavoring search engine competitors such as

[49] *See* European Commission Press Release IP/13/196, Commission fines Microsoft for non-compliance with browser choice commitments (Mar. 6, 2013), https://ec.europa.eu/commission/presscorner/detail/en/IP_13_196.

[50] Commission Decision of February 27, 2008, fixing the definitive amount of the periodic penalty payment imposed on Microsoft Corporation by Decision C (2005) 4420 final, 2009 O.J. (C 166). This fine was upheld but reduced to €860 million by the General Court. *See* James Kanter, *In European Court, a Small Victory for Microsoft*, N.Y. TIMES (June 27, 2012), https://nyti.ms/MAx1tU.

[51] Commission Decision of June 27, 2017, relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)) C (2017) 76, 213, available *at* https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.

[52] *See* Debra Cassens Weiss, *EU Punishes Google with Record $5.1B Antitrust Fine for Deals Requiring Preinstalled Apps, Services*, ABA JOURNAL (July 18, 2018, 8:48 AM), http://www.abajournal.com/news/article/eu_punishes_google_with_record_5.1b_antitrust_fine_for_deals_requiring_prei.

[53] *See* European Commission Press Release IP/18/4581, Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine (July 18, 2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581.

Microsoft and Yahoo.[54] In addition, the European Commission obtained commitments from Amazon in a case relating to e-books.[55]

C. Introduction to Data Protection Sanctions

Moreover, and more pertinent to our study, certain of the practices of the U.S. Tech Giants have also been subject to sanction by various EU Member State data protection authorities (DPAs),[56] called "supervisory authorities" in the GDPR,[57] and by other regulatory authorities even if they are not specifically in charge of data protection, such as competition authorities,[58] or financial authorities[59] such as the

---

[54] *See* European Commission Press Release IP/19/1770, Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising (Mar. 20, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

[55] *See* Summary of Commission Decision of May 4, 2017, relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.40153 — E-Book MFNS and related matters), 2017 O.J. (C 264) 7, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XC0811(02)&from=EN.

[56] *See, e.g.,* Houser & Voss, *supra* note 15, at 20–35.

[57] "Supervisory authority" is defined in the GDPR as "an independent public authority which is established by a Member State pursuant to Article 51." GDPR, *supra* note 1, art. 4(21). Pursuant to Article 51, it is charged with "monitoring the application of [the GDPR], in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the [European] Union." *Id*. art. 51(1). Note that this study will use the term "supervisory authority," or, alternatively, "DPA," to indicate this form of regulatory authority.

[58] *See* Commission Decision of May 17, 2017, Case M.8228 — *Facebook/WhatsApp*, notified under document C(2017) 3192; *see also Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data From Third-Party Sources is Abusive*, BUNDESKARTELLAMT (Dec. 19, 2017), *quoted in* PAUL FRIEDRICH NEMITZ, FINES UNDER THE GDPR 4–5 (2017) .

[59] *See, e.g.*, Financial Services Authority (U.K.), Final Notice to HSBC Actuaries and Consultants Limited, July 17, 2009 (regarding fines totaling over £ 3 million against companies of the HSBC), https://www.fca.org.uk/publication/final-notices/hsbc_actuaris0709.pdf; *see also* Financial Services Authority (U.K.), Final Notice to HSBC Life (UK) Limited (July 17, 2009), https://www.fca.org.uk/publication/final-notices/hsbc_inuk0907.pdf; *see also* Financial Services Authority (U.K.), Final Notice to HSBC Insurance Brokers Limited (July 17, 2009), https://www.fca.org.uk/publication/final-notices/hsbc_ins0709.pdf. For an additional example, *see also* Financial Services Authority (U.K.), Final Notice

UK Financial Services Authority.[60] Paul Nemitz refers to data protection and competition law both falling within "special economic administrative law,"[61] and the GDPR looks to competition law for the definition of "undertaking," used to determine the level of sanctions applicable in data protection enforcement actions.[62] However, many of the enforcement actions against the U.S. Tech Giants have been under the EU DP Directive,[63] the legislation that preceded and was repealed by the GDPR, and resulted in relatively small sanctions when compared to those in tax and competition law cases, and certainly when compared to the annual revenue of the U.S. Tech Giants. As an example, these could only go up to a maximum of €150,000 (for a first offense) in France; €900,000 in Spain, and £500,000 in the United Kingdom.[64]

One definition of "sanction" is "[a] provision that gives force to a legal imperative by either rewarding obedience or punishing disobedience."[65] Likewise, "sanctioning" has been defined as "the formal reaction to a violation of the law by the authorities" and it may be punitive or restorative.[66] Effective sanctions are seen as necessary for obtaining compliance with legal rules,[67] especially when people do not spontaneously comply with the rules because they consider them fair and deserving of respect for that reason alone. The imposing of sanctions is one tool of enforcement, as we have seen, and enforcement in turn is meant to put into application legal standards meant to

---

to Zurich Insurance Plc, UK branch, Aug. 19, 2010 (regarding a fine of ££2,275 million pounds against Zurich Insurance). On the latter fine, *see also* Nemitz, supra note 58, at 14.

[60] Nemitz, *supra* note 58, at 14–15.

[61] *Id*. at 3.

[62] GDPR, *supra* note 1, recital (150) (referring to TFEU arts. 101 and 102, the provisions regarding, respectively, illegal cartels and abuse of a dominant position).

[63] EU DP Directive, *supra* note 4.

[64] *See* Grant & Crowther, *supra* note 8, at 301.

[65] *Sanction*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[66] Miroslava Scholten et al., *The Proliferation of EU Enforcement Authorities: A New Development in Law Enforcement in the EU*, *in* LAW ENFORCEMENT BY EU AUTHORITIES: IMPLICATIONS FOR POLITICAL AND JUDICIAL ACCOUNTABILITY 1, 5 (Miroslava Scholten & Michiel Luchtman, eds., 2017).

[67] *See* Sebastian J. Golla, *Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines Under the GDPR*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 70, 70 (2017), (citing THOMAS RAISER, GRUNDLAGEN DER RECHTSSOZIOLOGIE 253 (Mohr Siebeck 6th ed. 2013)).

influence behavior.[68] Indeed, effectiveness of sanctions may be evaluated by first identifying the desired outcome, such as discouraging non-compliance, encouraging good practice, or raising awareness of privacy rights, for example,[69] and comparing this to the result achieved. However, it is more difficult to measure compliance with privacy laws than to measure enforcement.[70] Sanctions may take many forms beyond the basic carrot and the stick announced in the definition of the term. For example, there are criminal sanctions,[71] administrative sanctions,[72] and civil sanctions.[73] In addition, as various factors may need to be taken into account in the application of sanctions, their level may not be fixed once and for all but determined

---

[68] *See* David Wright & Paul De Hert, *Introduction to Enforcing Privacy*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 1, 2 (David Wright & Paul De Hert eds., 2016) (defining enforcement as "to translate a set of legal standards designed to influence human and institutional behavior into social reality" (citation omitted)).

[69] *See* Grant & Crowther, *supra* note 8, at 290.

[70] *See* Graham Greenleaf, *Responsive Regulation of Data Privacy: Theory and Asian Examples*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 233, 234 (David Wright & Paul De Hert eds., 2016) (commenting that enforcement may be measured by published national statistics and case studies, whereas few studies of compliance exist).

[71] A criminal sanction may be defined as "[a] sanction attached to a criminal conviction, such as a fine or restitution." *Criminal Sanction*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[72] In the United States, administrative sanctions have been upheld by courts "on the basis of the remedial or regulatory ingredients of the sanctions" (citations omitted), rather than the penal element of sanctions. *See* Lillian R. Altree, *Administrative Sanctions: Regulations and Adjudication*, 16 STAN. L. REV. 630, 632–33 (1964). In the European Union, administrative sanctions have taken several forms: "such as the loss of a deposit, the administrative fine, the surcharge, the exclusion from subsidies and blacklisting." *See also* Adrienne de Moor-van Vugt, *Administrative Sanctions in EU Law*, 5 REV. EUR. ADMIN. L. 5 (2012). This study is more focused on administrative *fines*, although other forms of sanctions are discussed as well.

[73] Grant and Crowther refer to a "civil penalty ordered by a court," in addition to administrative or criminal penalties. *See* Grant & Crowther, *supra* note 8, at 288.

on a case-by-case basis instead.[74] Furthermore, there are sanctions specific to various areas of law.[75]

The sanctions involved in the specific field of European Union data protection law are at the heart of this study, which is organized as follows: after this Introduction, Part I deals with the theory of sanctions and their goals as applied to EU data protection law. Part II of the study focuses on the nature of sanctions provided by the EU data protection law, starting with the EU DP Directive and continuing with the GDPR. Part III of the study analyzes the strategic risks involved in firms' lack of understanding of, and non-compliance with, the GDPR, and the risks of supervisory authorities' non-enforcement of the GDPR; Part IV provides recommendations both to firms and to the authorities in this regard. In Part V, conclusory remarks are made.

I. GOALS OF SANCTIONS

Before detailing the objectives of the sanctions that the DPAs of the European Member States may impose to enforce the GDPR, it is necessary to specify the nature of these sanctions: they are financial, administrative and regulatory. [76] First, the sanctions in question are financial sanctions, such as fines, as they consist of the relevant DPA obliging the sanctioned entities to pay a sum of money if they do not comply with the obligations provided by the GDPR.[77] The sums to be paid following a determination of a data protection violation by a regulatory authority must be paid into the budget of the nation where the sanction is imposed.[78]

---

[74] *See*, *e.g.*, U.S. Sentencing Guidelines Manual § 8C2.5 (f) (2018). *See also id*. ch. 8 (for chapter entitled, *Sentencing of Organizations: Introductory Commentary*, which states that "[. . .] The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, co-operation, or acceptance of responsibility.").

[75] For example, there may be compensation for harm for negligence or strict liability in torts law, as well as punitive damages; in contracts law there are expectation damages, but also potentially specific performance; in criminal law, punishment; under regulation, penalty sanctions, and so on. Robert Cooter, *Prices and Sanctions*, 84 COLUM. L. REV. 1523, 1538–51 (1984).

[76] Heinrich Amadeus Wolff, *The Implementation of Administrative Fines Under the General Data Protection Regulation from the German Perspective*, 2 INT'L J. FOR THE DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 11, 14 (2018).

[77] GDPR, *supra* note 1, art. 83.

[78] For example, for the United Kingdom, *see GDPR Penalties and Fines: Who Gets the Money from GDPR Fines?*, IT GOVERNANCE,

Secondly, these sanctions are administrative[79] because they are not imposed by courts as such but by administrative bodies.[80] More specifically, they are regulatory sanctions because the power to sanction given to DPAs is part of their regulatory powers.[81] Even if these sanctions are not criminal penalties, they are nevertheless criminal matters within the meaning of Article 6 of the European Convention on Human Rights (ECHR), guaranteeing a right to a fair trial.[82] Indeed, Article 83(8) provides, in a similar manner, that "[t]he exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance

---

https://www.itgovernance.co.uk/dpa-and-gdpr-penalties ("All fines collected by the ICO go to HM Treasury's Consolidated Fund to be spent on health and social care, education, policing and justice, and the like.") (last visited on Oct. 24, 2020); for France, *see* Julien Lausson, *Où va l'argent quand les géants de la tech paient des amendes?* [Where Does the Money Go When Tech Giants Pay Fines?], NUMERAMA (Nov. 3, 2019), https://www.numerama.com/politique/565914-ou-va-largent-quand-les-geants-du-net-paient-des-amendes.html ("ces montants, lorsqu'ils proviennent de décisions de la CNIL, sont versés au budget français" [these amounts, when they come from CNIL decisions, are paid to the French budget.]).

[79] *Article 29 Data Protection Working Party, Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679,* WP 253 (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 [hereinafter WP 253].

[80] Article 83(9) allows for the penalties for violations of the GDPR to be "initiated by the competent supervisory authority and imposed by competent national courts". *See* GDPR, *supra* note 1, art. 83(9). This provision is exceptional. Denmark and Estonia use this possibility, because they do not use administrative fines. *See also* Wolff, *supra* note 76, at 13; *See also,* GDPR, *supra* note 1, Recital 151.

[81] *See* GDPR, *supra* note 1, Recital 129. DPAs' powers are more extended than under the directive. *See* Philip Schütz, *The Set Up of Data Protection Authorities as a New Regulatory Approach* in EUROPEAN DATA PROTECTION: IN GOOD HEALTH? 1, 14 (S. Gutwirth, R. Leenes, P. de Hert & Y Poullet, eds., 2012) ("the Directive provides DPAs with investigative powers, effective powers of intervention and the power to engage in legal proceedings.").

[82] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 6, Nov. 4, 1950, 213 U.N.T.S. 221, 230. This Convention applies in the EU Member States and in the other nations of the Council of Europe. *See also Engel and others vs. The Netherlands*, 1976 Eur. Ct. Hr. 1, https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57479%22]}. *See also Oztürk vs. Germany*, 1984 Eur. Ct. Hr. 1, https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57552%22]}.

with Union and Member State law, including effective judicial remedy and due process."[83]

By their nature, the regulatory sanctions provided for in the GDPR are different from strictly criminal sanctions. Thus, criminal courts may use penalties of a different nature, such as fines, whereas DPAs may not order prison sentences at all.[84] Besides, malicious intention is not required for administrative sanctions.[85] Regulatory sanctions imposed on regulated entities are also distinct from the sanctions that may be imposed on the managers of regulated companies in person.[86] Regulatory sanctions are distinct from civil sanctions, particularly in the context of private enforcement, which allows victims to obtain damages to compensate for the harm they have suffered.[87] The primary purpose of regulatory sanctions is not the reparation, but rather the punishment of offenders.[88] The financial sanctions that DPAs may impose are also different from injunctions and other administrative or coercive measures such as the withdrawal of an administrative authorization or an obligation to implement a compliance program.[89] It is important to bear in mind that financial penalties imposed by DPAs on regulated companies may be in addition to or as an alternative to these other types of sanctions.[90]

---

[83] GDPR, *supra* note 1, art. 83(8).

[84] *See* Mitchel A. Polinsky & Steven Shavell, *The Optimal Use of Fines and Imprisonment*, 24 J. PUB. ECON. 89, 89–90 (1984). *See also* Cyrus Chu & Neville Jiang, *Are Fines More Efficient Than Imprisonment*?, 51 J. PUB. ECON. 391, 391–92 (1993).

[85] Intention is only a circumstance that must be taken into account when sentencing. *See* GDPR, *supra* note 1, art. 83(2)(b).

[86] *See* OECD, *Cartels: Sanctions Against Individuals,* 9(3) OECD J.: COMPETITION L& POL'Y 7, 10 (2007), https://read.oecd-ilibrary.org/governance/cartels-sanctions-against-individuals_clp-v9-art10-en ("As corporate sanctions rarely are sufficiently high to be an optimal deterrent against cartels, there is a place for sanctions against natural persons that can complement corporate sanctions and provide an enhancement to deterrence.").

[87] GDPR, *supra* note 1, art. 82 and Recitals 146–47.

[88] WP 253, *supra* note 79, at 6 ("The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish").

[89] JOHN BRAITHWAITE, RESTORATIVE JUSTICE AND RESPONSIVE REGULATION 29, 31 (2002).

[90] *See* GDPR, *supra* note 1, art. 83(2) ("Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or

The *raison d'être* for regulatory sanctions is specific, and it explains that there are regulatory sanctions in addition to other categories of sanctions that are typically criminal, civil, or administrative.[91] Regulatory sanctions can contribute to pursuing the same goals as other types of sanctions.[92] However, ultimately, regulatory sanctions aim to ensure the effectiveness of the whole legal framework that the supervisory authorities are responsible for enforcing.[93]

The functions of sanctions that are traditionally identified as criminal, civil, or administrative sanctions appear as sub-goals to ultimately achieve the key objective of compliance with the rules that European data protection legislation intends to promote and guarantee.[94]

In order to present the different goals that regulatory sanctions of DPAs can achieve, this study proposes to draw inspiration from the theories of sanctions and sentencing.[95] However, in order to streamline

---

instead of, measures referred to in points (a) to (h) and (j) of Article 58(2).”). Article 58(2) sets out the corrective powers of DPAs. *Id*. art. 58(2). On the various GDPR sanctions, *see also infra* Part II.

[91] *See* WP 253, *supra* note 79, at 4 (“Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures provided by article 58.”).

[92] S*ee* Ioannis Lianos et al., *An Optimal and Just Financial Penalties System for Infringements of Competition Law: A Comparative Analysis*, 27 CLES, Research Paper No. 3/2014, 2014, https://ssrn.com/abstract=2542991 (“From a legal standpoint, sanctions could pursue a number of other goals such as retribution, incapacitation, rehabilitation etc. Usually laws, and competition law is no exception, do not clearly specify what the goal of law enforcement is supposed to be. These goals are not necessarily in conflict with the goal of deterrence pursued by the economic approach.”).

[93] *See*, *e.g.*, Nemitz, *supra* note 58, at 2 (“Whether Article 83 GDPR can fulfil its function in practice will depend crucially on its implementation by the Data Protection Authorities: It will be essential that the supervisory authorities are adequately resourced in terms of infrastructure, personnel and finances in order to be able to fulfil their role, also vis-à-vis internationally and globally active companies, thus enabling the GDPR to be implemented and applied effectively”). *See also* Richard Macrory, *Reforming Regulatory Sanctions – Designing a Systematic Approach*, *in* THE REGULATORY STATE: CONSTITUTIONAL IMPLICATIONS 229, 230 (Dawn Olivier et al., eds., 2010).

[94] *See* GDPR, *supra* note 1, Recitals 11 & 129.

[95] *See*, *e.g.*, Henry M. Hart, Jr., *The Aims of the Criminal Law*, 23 LAW & CONTEMP. PROBS. 401, 404–05 (1958). *See also* Julian V. Roberts & Andrew Von Hirsch, *Legislating the Purpose and Principles of Sentencing*, *in* MAKING

the presentation of these different functions and to highlight the specific issues attached to these sanctions, this study proposes an original analytical framework. This framework is based on a double distinction with regard to the functions of sanctions. First, we distinguish between the symbolic and material functions of sanctions,[96] and secondly, we distinguish between the retrospective (backward-oriented) and prospective (forward-oriented) natures of sanctions.[97]

A sanction always has content. It consists, for example, of depriving a person of his or her liberty, forcing him or her to pay a certain amount of money or to perform a certain action. This content can be said to be material. The materiality of the sanction is obvious when the sanction is a fine. As such, the sanction aims at changing something in the state of the world (by a transfer of wealth, by a remedial measure, etc.).[98] But the sanction also has a meaning independently of its content, by the very fact that it is a sanction: this is the symbolic aspect of the sanction.[99] The sanction is, in fact, a

---

SENSE OF SENTENCING 48, 51 (J. V. Roberts & D.P. Cole, eds., 1999); *See generally,* MICHAEL TONRY, WHY PUNISH? HOW MUCH? A READER ON PUNISHMENT (2011); *See also* ALFRED BLUMSTEIN, *Making Sentencing Policy More Rational and More Effective*, 25 ISR. L. REV. 607, 608 (1991); *See also* PAMALA L. GRISET, DETERMINING SENTENCING. THE PROMISE AND THE REALITY OF RETRIBUTIVE JUSTICE 3 (1991) ("the four traditional purposes of the criminal sanction: rehabilitation, incapacitation, deterrence, and retribution").

[96] This study notes that this distinction does not cover the distinction between monetary and non-monetary sanctions. A sanction such as imprisonment is not monetary, but it is not purely symbolic! A monetary sanction can be essentially symbolic; if the amount is very small, especially in view of the financial capacity of the person sanctioned.

[97] *See* Mustapha Mekki, *Considérations sociologiques sur le droit des sanctions* [Sociological Considerations on the Law of Sanctions], *in* LES SANCTIONS EN DROIT CONTEMPORAIN. LA SANCTION, ENTRE TECHNIQUE ET POLITIQUE [SANCTIONS UNDER CONTEMPORARY LAW: PUNISHMENT-BETWEEN TECHNIQUE AND POLITICS] 31, 33–34 (C. Chainais & D. Fenouillet, eds., 2012).

[98] Cécile Chénais & Dominique Fenouillet, *Le droit contemporain des sanctions, entre technique et politique* [*Contemporary Law of Sanctions, Between Technique and Politics*], *in* LES SANCTIONS EN DROIT CONTEMPORAIN. LA SANCTION, ENTRE TECHNIQUE ET POLITIQUE [SANCTIONS UNDER CONTEMPORARY LAW: PUNISHMENT- BETWEEN TECHNIQUE AND POLITICS] XI, LXXIX, n°88 (C. Chainais & D. Fenouillet, eds., 2012).

[99] The symbolic dimension of social and economic interactions was emphasized by Marcel Mauss in his essay on the gift. There is, of course, an economic value that is transferred in the gift and counter-gift transactions he

message addressed to the person sanctioned and, beyond the offender, to other persons who might be affected by the rule.[100] This message does not aim to change the state of the world, at least not immediately, but it does aim to change some representations of the world. The symbolic effect is not necessarily linked to the importance of the content of the sanction. Thus, a sanction whose content is very light may nevertheless have a meaning: the fact of being condemned sometimes is more important than the magnitude of the condemnation. However, the importance of the sanction can sometimes also be a message that has a meaning (denunciation function). Even if a sanction is ultimately not applied (for example, because it cannot be applied, if the sum to be paid exceeds the financial capacity of the person sanctioned), the fact that the sanction is heavy is a message from the sanctioning judge or authority to citizens.[101]

On the other hand, sanctions may seek to produce effects in relation to a past situation or in relation to a future situation.[102] There are thus backward-oriented sanctions and forward-oriented sanctions.[103] For example, a sanction may aim to react to a past act. Since an act is deemed to be wrong because it is contrary to the law, [104] it infringes legally protected interests, or it constitutes a social disorder, the role of the legal procedure and, ultimately of the sanction, is to counteract this act, erase its consequences and punish the perpetrator of the act. The ideal is to be able to restore the status quo disturbed by the non-compliant act. Sanctioning does not always achieve this ideal because events are often irreversible, at least partially irreversible. But

---

describes, but the social significance of this act makes the economic and material aspect of the transfer a very secondary one. MARCEL MAUSS, ESSAI SUR LE DON: FORME ET RAISON DE L'ÉCHANGE DANS LES SOCIÉTÉS ARCHAÏQUES, *translated in* MARCEL MAUSS, THE GIFT: FORMS AND FUNCTIONS OF EXCHANGE IN ARCHAIC SOCIETIES, 42-84 (W.D.Halls, trans., 1990), https://libcom.org/files/Mauss%20-%20The%20Gift.pdf. The concept of symbolic sanction can be used by scholars when the effectiveness of the sanctions is doubtful, as it is the case in the field of international economic sanctions. *See* Taehee Wang, *Playing to the Home Crowd? Symbolic Use of Economic Sanctions in the United States*, 55 INT'L STUD. Q. 787, 788 (2011).

[100] Antony R. Duff, *Punishment, Retribution and Communication*, *in* PRINCIPLED SENTENCING READINGS ON THEORY AND POLICY 126, 126–27 (Andrew von Hirsh, Andrew Ashworth & Julian Roberts, eds., 2009).

[101] JOEL FEINBERG, DOING AND DESERVING 100 (1970).

[102] John M. Darley, Kevin M. Carlsmith and Paul H. Robinson, *The Ex Ante Function of Criminal Law*, 35 LAW & SOC'Y REV. 165, 165–66 (2001).

[103] *Id*.

[104] Mekki, *supra* note 97, at 33.

an important function of sanctions is to make the response to an offense as relevant and effective as possible. Restoring the status quo in line with the law is one way of ensuring the effectiveness of the norm through an adequate response. Conversely, the purpose of a sanction may be to prevent the future occurrence of an act contrary to law. In this case, the relevant sanction is not the one imposed on the perpetrator of a concrete behavior, but the one that abstractly threatens those who would break the law. A sanction applied to a particular person for a past offense may also produce effects in the future for that person (the aim is to prevent him or her from repeating the offense) or for others because the sanction imposed is designed to be exemplary.[105] The sanction has a preventive function if it prevents or hinders the future performance of an offense or if it effectively persuades persons that it is better not to commit an offense in view of the sanction incurred in that case.[106]

The two criteria can be combined, and the different functions of sanctions can therefore be put into the following matrix.

Effects of the Sanctions	**Symbolic**	**Material**
Backward-oriented	Retribution Rehabilitation	Reparation Confiscatory
Forward-oriented	Expressive function Normative function	Deterrence Incapacitation

This study will examine these different sub-goals to show whether, how, and under what specific conditions the sanctions imposed, or likely to be imposed, by DPAs can contribute to make the GDPR effective. In particular, this study will consider whether the sanctions must be effective in order to play their role, whether they must be heavy in order to be effective, and whether they must be consistently applied by DPAs in order for the GDPR to be properly

[105] Anthony Bottoms and Andrew Von Hirsch make a distinction between "special deterrence" ("reformation" in Bentham's wording) and "general deterrence" (example), for instance. *See* Anthony Bottoms & Andrew Von Hirsch, *The Crime Preventive Impact of Penal Sanctions*, *in* THE OXFORD HANDBOOK OF EMPIRICAL LEGAL RESEARCH 96, 97 (P. Cane and H. M. Kritzner, eds., 2010). *See also* PATRICK MORVAN, CRIMINOLOGIE [CRIMINOLOGY] 309 (2019).

[106] *See* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 4 (1990, Princeton University Press ed., 2006) ("An instrumental perspective regards compliance as a form of behavior occurring in response to external factors. It leads to a focus on the extent and nature of the resources that authorities have for shaping public behavior [by contrast to a normative perspective studied by the author].").

enforced. First, this study will investigate the retribution and rehabilitation functions of sanctions (Section A). Then, the confiscation and reparation functions are detailed (Section B), after which this study delves into the expressive and normative goals of sanctions (Section C). Finally, the deterrence and incapacitation functions of sanctions are analyzed (Section D), before conclusory remarks on the theory of sanctions (Section E).

A. Retribution and Rehabilitation

This Part of the study investigates the retribution function (Section 1), prior to studying the rehabilitation function (Section 2).

1. Retribution

The most obvious function of punitive sanctions is that of retribution.[107] The sanction responds *prima facie* to a request for a symbolic reaction. An evil has been done; in return, an evil must be applied to the one who committed the initial evil.[108] Punishment is a response to the transgression. A sanction, regardless of its content, is therefore first of all an official acknowledgement that an evil has been committed.[109]

The retributive compensation may take the form of an obligation to pay a certain amount of money (fine) or to lose control of property (confiscation).[110] But the sanction can also be immaterial.[111] Infamous sanctions or making the sanction public is an accessory or principal penalty in criminal law, and even more in a regulatory approach through "publicity order" for instance.[112] Such sanctions are

---

[107] Gerard V. Bradley, *Retribution: The Central Aim of Punishment*, 27 HARV. J.L. & PUB. POL'Y 19, 24 (2003–2004).

[108] *Immanuel Kant*, *The Penal Law and the Law of Pardon*, *in* THE METAPHYSICAL ELEMENTS OF JUSTICE 331 (1999), *quoted in* Tonry, *supra* note 95, at 31.

[109] Micheal S. Moore, *The Moral Worth of Retribution*, *in* PRINCIPLED SENTENCING: READINGS ON THEORY AND POLICY 110 (A. von Hirsch et al., eds, 1987).

[110] *See* Jean-Paul Céré & Ludivine Grégoire, *Peine (Nature et prononcé), in* REPERTOIRE DE DROIT PENAL ET DE PROCEDURE PENALE (2020).

[111] See Golla, *supra* note 67, at 70 ("Even though immaterial damages such as loss of reputation due to a mention in an activity report or a high-damage claim can be more painful for an enterprise in certain cases, technically administrative fines and criminal penalties are to be regarded as the most severe sanctions for data protection violations.").

[112] Richard Macrory, *New Approaches to Regulatory Sanctions*, 20 ENVTL. L. & MGMT. 210, 212 (2008).

also provided for in data protection law.[113] The regulator may make public with varying degrees of force the GDPR violation and the infringement of data subject rights.[114] A regulator may thus choose to display information prominently on its website, communicate to the media and the public through press releases, or even generate discussion about a sanction through press interviews.[115] When the entity that is sanctioned is a media, it may be condemned to inform its users of the sanction that has been imposed on him.[116] The more a company depends on its reputation, the more redoubtable these kinds of sanctions will be for it.[117] Many companies collecting personal data are strongly impacted by attacks on their image in the users' eyes. Companies whose clients are other companies may be less sensitive to this. Scandals concerning the illegal exploitation of personal data or the lack of security of sensitive data show the vulnerability of companies

[113] GDPR, *supra* note 1, art. 58 (a) and (b).

[114] The sanction pronounced by the French CNIL against Google is an illustration of a deliberate decision by the regulatory authority to "make public." *See* Deliberation No. SAN-2019-001 of the Restricted Committee of the CNIL (Jan. 21, 2019) pronouncing a financial sanction against financial sanction against Google LLC. at 28, https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf ("The Restricted Committee of the CNIL, after having deliberated, decides . . . to make its decision public on the CNIL website and on the Légifrance website, which will be anonymized upon expiry of a period of two years from its publication.").

[115] *See* Golla, *supra* note 67, at 71 ("Even though immaterial damages such as loss of reputation due to a mention in an activity report or a high-damage claim can be more painful for an enterprise in certain cases, technically administrative fines and criminal penalties are to be regarded as the most severe sanctions for data protection violations.").

[116] Thierry Kirat, Frédéric Marty, Hugues Bouthinon-Dumas & Amir Rezaee, *Quand dire c'est réguler* [*When to Say is to Regulate*], 25 ÉCONOMIE ET INSTITUTIONS 3 (2017).

[117] In a prior enforcement action regarding Google's privacy policy, this was arguably the case. In that instance, the CNIL also pronounced a sanction that included a publicity element, which required publication of a notice on Google's home page. *See* W. Gregory Voss, *European Union Data Privacy Law Developments*, 70 BUS. LAW. 253, 255 (2014/2015) ("a decision … requiring the publication of a communique regarding the fine and data breaches, as well as linking the decision, for a period of forty-eight consecutive hours, on its French home page. The publication sanction was perhaps the most prejudicial (at least from an image standpoint) to Google") (citation omitted).

in this respect.[118] In view of the retributive function of the sanction, companies can expect to be sanctioned whenever they violate the regulation, and the regulatory authorities know it, and they must fear being sanctioned all the more severely when the breaches are serious. The application of sanctions according to the logic of the giving and receiving principle, basically founded on the law of retaliation, is reinforced by the principle of proportionality included in the European law about sanctions.[119] The requirement laid down in the GDPR, in particular in its Article 83(1), that penalties must be "effective, proportionate and dissuasive," [120] is interpreted most of the time from a quantitative perspective (that is the material aspect of the penalty): there must be a relationship between the fault and/or the harm to the interests of others, on the one hand, and the magnitude of the penalty, on the other.[121] But the requirement of proportionality may also suggest a symbolic interpretation: an offense must give rise to a sanction in reaction, just as a donation calls for a counter-gift.[122]

2. Rehabilitation

The retributive function is linked to the symbolic part of the rehabilitative function or psychological effect of the sanction.[123] The sanction is not only a message about the wrong act; it also implies consequences for the way in which the offender and possibly the victims of the offense (if there are any) are viewed.[124] In ordinary criminal law, particularly in the context of the punishment of offenses against persons, the rehabilitative function of the victims is

---

[118] Yasmine Agelidis, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them,* 31 BERKELEY TECH. L.J. 1057, 1069 (2016).

[119] Morris J. Fish, An *Eye for an Eye: Proportionality as a Moral Principle of Punishment*, 28(1) OXFORD J. LEGAL STUD. 57, 58 (2008).

[120] GDPR, *supra* note 1, art. 83(1) ("Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive." The cited paragraphs refer to the levels of administrative fines for various infringements.).

[121] *See* WP 253, *supra* note 79, at 6.

[122] Mauss, *supra* note 99, at 50.

[123] Mekki, *supra* note 97, at 48–49.

[124] ANTOINE GARAPON, BIEN JUGER: ESSAI SUR LE RITUEL JUDICIAIRE [GOOD JUDGMENT: ESSAY ON THE JUDICIAL RITUAL] 63–65 (1997). *See also* MICHEL FOUCAULT, SURVEILLER ET PUNIR [DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON] 14 (1977).

important.[125] For example, it seems important that the victim of a rape who might paradoxically feel a sense of guilt should be regarded as a victim thanks to the punishment.[126] Such a consideration may play a certain role in the field of data protection. It may be important that users who have had their sensitive data misappropriated as a result of a breach of data security obligations on the part of the data controller are told that this harm is not the result of their own negligence but the effect of a breach of the regulation which for this reason deserves a sanction. The *Ashley Madison* case,[127] in which a dating platform for extramarital relationships did not ensure the security of this obviously very sensitive data[128] for the data subjects, illustrates this problem.

The rehabilitative function also concerns the offender.[129] Being punished is seen in classical sentencing theory as a necessary step for the offender to transform himself or herself to become someone different from the one who may have committed the offense.[130] In theory, the rehabilitation of the offender, that can be included in the restorative justice approach, including for white-collar crime,[131] does

---

[125] *See* Mary Margaret Giannini, *Equal Rights for Equal Rites?: Victim Allocution, Defendant Allocution, and the Crime Victims' Rights Act*, 26 YALE L. & POL'Y REV. 431, 449 (2007).

[126] Tyler G. Okimoto & Michael Wenzel, *Punishment as Restoration of Group and Offender Values Following a Transgression: Value Consensus Through Symbolic Labelling and Offender Reform*, 39 EUR. J. SOC. PSYCHOL. 346, 348 (2008).

[127] On the Ashley Madison case, where hackers obtained sensitive data on users of the site, *see* Dino Grandoni, *Ashley Madison, A Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (Jul. 20, 2015), https://nyti.ms/1Jc7acr.

[128] The GDPR category of sensitive data or "special categories of personal data," specifically includes "data concerning a natural person's sex life." GDPR, *supra* note 1, art. 9(1).

[129] *See* Céré & Grégoire, *supra* note 110, at nos. 8–9.

[130] MARC ANCEL, LA DEFENSE SOCIALE NOUVELLE, UN MOUVEMENT DE POLITIQUE CRIMINELLE HUMANISTE [THE NEW SOCIAL DEFENSE, A HUMANIST CRIMINAL POLICY MOVEMENT] (1954); PIERRE LALANDE, PUNIR OU REHABILITER LES CONTREVENANTS ? DU NOTHING WORKS AU WHAT WORKS (MONTEE, DECLIN ET RETOUR DE L'IDEAL DE REHABILITATION) [PUNISH OR REHABILITATE OFFENDERS? FROM NOTHING WORKS TO WHAT WORKS (RISE, DECLINE AND RETURN OF THE REHABILITATION IDEAL)] 30–77, Ministère de la sécurité publique du Canada (2006).

[131] JOHN BRAITHWAITE, CRIME, SHAME AND REINTEGRATION 125 (1989) ("Seventeen cases were studied (on the basis of interviews with executives and other sources) in which corporations had been through adverse publicity crises. The financial impacts of adverse publicity (on sales, earnings, stock

not necessarily require a heavy sanction.[132] In the field of criminal or regulatory law that applies to companies, this function of punishment plays a very limited role.[133] The transformation of the company that violates the GDPR requires more than a symbolic monetary sanction, as we shall see with regard to the incapacitation function.[134]

With regard to the retributive and rehabilitative role that sanctions under the GDPR can play, it can be concluded that, if breaches of the law can be identified, it is important that they do not remain unpunished and therefore, that sanctions are effectively and even systematically applied (at least if other regulatory responses remained insufficient). As this function is symbolic, it is not necessary for sanctions to be severe (but sanctions may need to be severe for other reasons).[135] In addition, in order for the functions of retribution and rehabilitation to be fulfilled, it is important that the sanctions are properly enforced by all DPAs. If there is a jurisdiction in Europe where the DPA is reluctant to react to violations or reacts very slowly compared to other DPAs, this may send the problematic message that violations go unpunished in that territory. This may logically lead to companies that tend to be non-compliant to preferentially locate in the territory of that authority, through what may be described as a form of forum-shopping. This is the problem that a jurisdiction such as Ireland could raise, if it appears that it does not apply sanctions, even symbolic ones, to companies that deserve to be punished.[136] As we shall see, while from a strictly symbolic point of view, light sanctions are more useful than no sanctions at all, there are other reasons to consider that

---

prices, etc.) were generally found to be slight; however, nonfinancial impacts on the loss of repute which executives perceived their company and themselves to have suffered in the community were found to be important to them".). *Id.* at 124.

[132] *See* GDPR, *supra* note 1, Recital 148.

[133] It is the case as far as fines can be viewed as a "cost of doing business." *See* Leonard Orland, *Reflections on Corporate Crime: Law in Search of Theory and Scholarship*, 17 AM. CRIM. L. REV. 501, 516 (1979–1980).

[134] *See infra* Section D.2.

[135] Recent developments in criminal policy show that public authorities want a systematic "criminal response" when offenses are proven, even if there is no need to apply sanctions in the strict sense. In the French context, *see* Laura Aubert, *Systématisme pénal et alternatives aux poursuites en France: une politique pénale en trompe-l'œil* [*Criminal System and Alternatives to Prosecution in France: A Criminal Policy in Trompe l'oeil*], 74(1) DROIT ET SOCIETE 17–33 (2010).

[136] Joshua Blume, *A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR*, 49 GEO. J. INT'L L. 1425, 1455 (2018).

light sanctions against powerful actors prevent other functions of sanctions from being fulfilled.[137]

B. Confiscation and Reparation

The penalty imposed on the perpetrator of an offense does not merely serve to declare that an offense has been committed. It can also be used to repair the situation, or the relationship, disrupted by the offense. Reparation can be applied to three categories of actors and refers more specifically to three sub-goals, that this study sets out as confiscation (Section 1), reparation (Section 2), and a financing function (Section 3).

1. Confiscation

First, for the offender, reparation consists in removing the positive consequences that the offense may have generated on his or her economic situation. The sanction must then result in the deprivation of the benefit of the offense.[138] The financial penalty is convenient to play this role of confiscation of an illegitimate profit.[139] This implies, for example, that the sanction should be at least as high as the unlawful profit. This approach is common in other branches of economic criminal law such as competition law or market abuse law. Sentencing rules generally take into account the illegitimate profit. For example, the amount of the benefits derived from the offense is the minimum amount of the fine or the fine is a multiple of the illicit profit.[140] This

---

[137] *See infra* Sections B.1 (on the confiscation function), B.3 (on the financing function), C.1 (on the expressive function), and above all D.1 and D.2 (on the deterrence and incapacitation functions). All of these functions require heavy penalties imposed on large corporations (such as the U.S. Tech Giants, when they violate data protection law), virtually or effectively.

[138] Claude Ducouloux-Favard, *L'amende dans son rapport avec le profit* [The Fine in Relation to Profit], *in* LA CRIMINALITE D'ARGENT: QUELLE REPRESSION? [FINANCIAL CRIME: WHAT REPRESSION?] 183, 184 (C. Ducouloux-Favard & Ch. Lopez, eds., 2004) (explaining that legislation setting out scales of fines for illegal profit are one of two types: either the legislator allows fines to exceed the scale's maximum when the illegal profit itself exceeds that maximum; or it requires that the fine be at least equal to the profit derived from the crime).

[139] Macrory, *supra* note 112, at 211.

[140] *See*, *e.g.*, Lianos et al., *supra* note 92, at 9 ("According to economic theory, fines should be at least equal to the expected illegally earned profits divided by the probability to be caught, hence they should relate to expected profits originating from the violation and not to the profits actually gained that may be higher or lower than those expected at decision-making time, should the fines be paid after the period of infringement").

approach can be applied in the data area. In today's economy, data have a high economic value and are the main source of wealth for tech giants.[141] The additional data that could be collected and processed by companies in violation of the GDPR could bring them additional profit, which in this case would be illegal.[142] The GDPR refers to "financial benefits" that must be taken into account in determining the amount of the penalty that the DPA could apply to a non-compliant company.[143]

2. Reparation

The sanction may theoretically be intended, among other things, to compensate for the harm suffered by particular victims. It is clear that this function is not fulfilled by financial sanctions imposed by DPAs because the amounts to be paid by the sanctioned entity are not paid to the victims. It is the civil action that provides adequate compensation to the victims.[144] Indeed, this is the main purpose of the civil liability mechanism.[145] The concern to provide victims with compensation for their losses is not at all absent from the GDPR, but it is referred to in Article 82[146] and not in Article 83, which is devoted to administrative penalties.[147] Regulatory sanctions do not contribute

---

[141] *See*, *e.g.*, Nemitz, *supra* note 58, at 1–7 ("They ensure that efforts of compliance are undertaken in addition to pure profitability investments and a fortiori that the economic advantage that controllers or processors derive from infringements of GDPR, if any, do not remain with them . . .[.[t]he amount of the fine must be significantly higher than any profit derived from the violation of the GDPR").

[142] Katharine Kemp, *Here's How Tech Giants Profit from Invading Our Privacy, and How We Can Start Taking it Back,* The Conversation (Aug. 11, 2019 4:03 PM EDT), https://theconversation.com/heres-how-tech-giants-profit-from-invading-our-privacy-and-how-we-can-start-taking-it-back-120078.

[143] GDPR, *supra* note 1, art. 83(2)(k).

[144] *Id*. art. 79(1) ("each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.").

[145] *See* Jean-Sébastien Borghetti, *Les sanctions en droit de la responsabilité civile* [*Sanctions in Civil Liability*], *in* LES SANCTIONS EN DROIT CONTEMPORAIN. LA SANCTION, ENTRE TECHNIQUE ET POLITIQUE [SANCTIONS UNDER CONTEMPORARY LAW: PUNISHMENT- BETWEEN TECHNIQUE AND POLITICS] 257, 259 (C. Chainais & D. Fenouillet, eds., 2012).

[146] *Id*. art. 82(1) ("Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.").

[147] *Id*. art. 83.

directly to this, even if the importance in duration and number of persons affected by the infringements are part of the criteria for determining the administrative penalty.[148] The sanction imposed by the regulator may simply facilitate private enforcement in parallel with the procedure before the regulatory authority, by facilitating the proof of the fault of the sanctioned entity.[149] In this respect, regulatory financial sanctions, if they are imposed, whatever the magnitude of the fine, facilitate private enforcement more than negotiated procedures that generally preclude admission of guilt.[150]

3. Financing Function

Thirdly, sanction can be conceived as a means of repairing the damage caused to the economy or society in general, irrespective of the particular harm.[151] Insofar as the amount of the fines is paid to collective budgets or to the regulatory authority, sanctions help to replenish public financial resources that can be used for projects of general interest (education of citizens, guarantee fund, etc.).[152] The sums collected by way of administrative sanctions, if paid into the general budget of the Member States, are not specifically earmarked

---

[148] *Id*. art. 83(2)(a). It may be noted that the damage suffered by the victims is included as part of the first criterion in the list of elements to be taken into account.

[149] *See, e.g.*, Nemitz, *supra* note 58, at 3 ("Private enforcement and actions for damages, even where special legislation for that purpose exists, play a smaller role, with the later often being efficient only as a follow on of public enforcement findings of illegality").

[150] The sanction decision pronounced by a regulatory authority facilitates the demonstration of a fault entitling the victim to compensation when the sanctioned violation is the cause of a particular prejudice. This has been underlined in particular by the European Court of Justice in the field of competition law (Mar. 9, 1978, *Simmenthal*, 106/77, Rec. 629, para. 16, and of June 19, 1990, *Factortame and others*, Case C-213/89, Rec. I-2433, para. 19). *See* Robert Saint-Esteben, *La reparation d'un préjudice économique resultant d'infractions au droit de la concurrence*, Conference held at the French Cour de Cassation, n°9, https://www.courdecassation.fr/IMG/File/pdf_2007/26-04-2007/26-04-2007_st_esteben.pdf.

[151] *See* Saint-Esteben, *supra* note 150, at no. 4.

[152] *See*, *e.g.*, the answer of the French Financial Markets Regulator (AMF) to the question "To whom are the pecuniary penalties imposed by the Enforcement Committee paid?" *Sanctions & transactions: FAQ: La sanction*, AMF, https://www.amf-france.org/fr/sanctions-transactions/faq/la-sanction#ancre-62499 (last visited on Oct. 27, 2020).

for personal data protection policy, but it is a political choice that can be made by EU Member States.[153]

Incidentally, sanctions can thus fulfil a funding function. Sanctions have an objective funding function when the cumulative amount of sanctions represents a significant financial flow for the State, EU or regulator's budget. This sanction function is often ignored by the theorists because it would be inadequate if the financing of public expenditure or even the functioning of a regulatory authority depended on sanctions, as this would mean that the normal functioning of institutions is based on the anticipation of deviant behavior on the part of regulated people.[154] One can note that a good sanction, and therefore good regulation, meant that sanctions did not have to be applied because regulated operators comply with the law. When sanctions were low and few in number, fines were not a significant source of funding for public institutions. But once the penalties incurred are very severe and the penalty-imposing authorities no longer hesitate to fine offending companies hard, penalties become a significant source of auxiliary funding.[155] In the field of competition law, for example, it has been observed that the cumulative amount of sanctions imposed by the European Commission has increased by a factor of twenty in 25

---

[153] One way of choosing to earmark the sums collected for personal data protection policy is to allocate the fines not to the general state budget but to the budget of the regulatory authorities (if they have budgetary autonomy). *See* Julien Lausson, *Où va l'argent quand les géants de la tech paient des amendes?* [Where Does the Money Go When Tech Giants Pay Fines?], NUMERAMA (Nov. 3, 2019), https://www.numerama.com/politique/565914-ou-va-largent-quand-les-geants-du-net-paient-des-amendes.html.

[154] *See*, *e.g.*, Matt Ford, *The Problem With Funding Government Through Fines*, ATLANTIC (Apr. 2, 2015), https://www.theatlantic.com/politics/archive/2015/04/the-problem-with-funding-government-through-fines/389387/.

[155] According to the Commission, "Fines imposed on companies found in breach of EU/EEA antitrust rules are paid into the general EU budget. This money is not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly. The fines therefore help to finance the EU and reduce the burden for taxpayers." *See* European Commission Press Release IP/20/1774, Antitrust: Commission fines car parts suppliers of € 18 million in cartel settlement (Sept. 29, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1774.

years.[156] Some antitrust sanctions exceed €1 billion.[157] As multi-billion-dollar fines could be imposed on large digital companies, sanctions in personal data protection law could become an interesting source of financing for States that are facing significant budgetary difficulties. This budgetary consideration tends to convince regulators not to hesitate to impose severe sanctions.[158] Thus, DPAs that would be quick to sanction in order to be the priority beneficiaries of the amount of the sanctions create the risk of opportunistic use of the power to sanction, motivated by funding considerations.[159] The case of the sanction pronounced by the French regulator, (CNIL) against Google, and confirmed by the judge competent to exercise judicial review, the French Council of State (Conseil d'Etat), may be examined in the light of this remark.[160] However, this creates a perverse incentive because the amount of the sanctions may be set for reasons other than those

---

[156] According to the European Union, "The EU's sources of income include contributions from member countries, import duties on products from outside the EU and fines imposed when businesses fail to comply with EU rules." *How the EU is Funded*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/eu-budget/revenue-income_en (last visited on Oct. 27, 2020). *See also* Matthew Keep, A Guide to EU Budget, UK House of Commons Briefing paper n°05455, at 3, file://hecate/myfiles/bouthinondumas/Downloads/SN06455.pdf.

[157] *See*, *e.g.*, Business Insider España, *The 7 Biggest Fines the EU Have Ever Imposed Against Giant Companies*, BUS. INSIDER (July 19, 2018, 8:11 AM), https://www.businessinsider.fr/us/the-7-biggest-fines-the-eu-has-ever-imposed-against-giant-corporations-2018-7.

[158] Unless the attraction or retention of foreign companies on the territory of a Member State is seen as a more important political priority objective than the replenishment of the State's coffers. The case of the Commission's sanction against Apple for the taxes that the company should have paid, according to the Commission (before being contradicted by the Court of First Instance), shows that Ireland did not seek to take opportunistic advantage of a decision that potentially brought it more than €13 billion, but made common cause with Apple to maintain its status as a welcoming territory for US tech giants. *See* Eugene Stuart, *Whether or Not to Bite the Apple: Some Implications of the August 2016 Commission Decision on Irish Tax Benefits for Apple*, 16(2) EUR. STATE AID L. Q. 209, 229 (2017).

[159] David Cowan, *Total GDPR Fines Climb to €114m as Companies Struggle to Comply with Regime,* THE GLOBAL LEGAL POST (Jan. 31, 2020), https://www.globallegalpost.com/corporate-counsel/total-gdpr-fines-climb-to-114m-as-companies-struggle-to-comply-with-regime-67962582/.

[160] For a discussion of this case, *see infra* Part II.

relating to the effective application of the regulation.[161] For this reason, it seems desirable that the policy for the application of sanctions be harmonized between the DPAs, in particular to ensure that the remedial function of sanctions is not misused. The adequate remedy to prevent the risk of a race towards administrative sanctions to finance the various EU Member States would be to substitute a sanction procedure conducted by the European Commission or the EDPB rather than by the national DPAs, or to allocate the amount of the sanctions imposed by the regulatory authorities to the EU budget, as is the case with fines for major anti-competitive practices.[162]

C. Expressive and Normative Goals

Sanctions play an important role in shaping the mental representations of individuals and companies, especially expectations of what might happen to them if they behave this way or that way.[163] The main effects of sanctions for the future are prevention and deterrence. But there is also a future-oriented symbolic effect of sanctions.[164] It corresponds to the expressive or denunciatory function (Section 1), as well as the normative function of sanctions (Section 2).

---

[161] It was observed that the large fines that some large companies had to pay represented a quite major contribution to the European budget. *See*, *e.g.*, William Watts, *Google's $2.7 Billion Goes into EU's Budget — And That's More Than Most Member Nations Put it*, MarketWatch (June 28, 2017, 2:43 AM ET), https://www.marketwatch.com/story/how-googles-27-billion-fine-stacks-up-against-each-eu-countrys-annual-budget-contribution-2017-06-27.

[162] Fines paid to the European budget lead to a reduction in Member States' contributions in proportion to their participation in the EU budget. *See Antitrust: Commission Fines NBCUniversal €14.3 Million for Restricting Sales of Film Merchandise Products*, EUROPEAN COMMISSION (Jan. 30, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_157 ("Fines imposed on companies found in breach of EU antitrust rules are paid into the general EU budget. This money is not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly.").

[163] Olivier Chassaing, *La portée normative des interdictions pénales* [*The Normative Scope of Criminal Prohibitions*], 93(1) RUE DESCARTES 28, AT NO. 16 (2018) ("La première fonction sociale de la loi pénale est de poser des modèles de conduites et d'adresser des interdictions pour les citoyens; elle ne sert à qualifier les situations punissables et à sanctionner les infracteurs que dans un second temps" [The first social function of criminal law is to lay down models of conduct and to issue prohibitions for citizens; it only serves to qualify punishable situations and to punish offenders in a second stage]).

[164] *See* Mekki, *supra* note 97.

1. Expressive Function

The mere fact that there is a sanction for transgression and that this sanction is a punishment, is a means of sending the message that the rules underlying this sanction are mandatory.[165] It promotes the awareness that these obligations and prohibitions must be complied with because it is law and more specifically hard law.[166] Citizens who spontaneously respect the legal order (or because they fear the stigmatizing effect of a criminal conviction for instance)[167] will thus be encouraged to comply with these rules because they know, namely via the sanctions, that the rules must be applied. This purely symbolic function of sanctions is, however, unlikely to significantly influence rational economic actors who tend to weigh costs and benefits related to compliance and non-compliance, according to the classical assumptions of Economic Analysis of the Law.[168] Besides, the level of sanctions incurred indicates the importance of these rules and the rights protected.[169]

---

[165] The rule is mandatory because it is sanctioned. To take up Henri Motulsky's concepts *see* HENRI MOTULSKY, PRINCIPES D'UNE RÉALISATION MÉTHODIQUE DU DROIT PRIVÉ [Principles of a Methodical Realization of Private Law] 18–19 (2002) (the rule is composed of two parts: the presupposition or hypothesis and the effect, i.e. the consequence implied by the hypothesis. If a sanction is incurred in the event of the performance of a certain conduct, this means that this conduct is legally prohibited and that it is obligatory not to perform this act. Similarly, if a sanction is provided for in the event of a breach of an obligation, this means that the obligation is legally binding!). *See* Bruno Oppetit, *Henri Motulsky et la philosophie du droit*, 38 ARCHIVES DE PHILOSOPHIE DU DROIT 251, 254 (1993) (Commenting that the rule of law has a necessarily coercive character and that it implies an at least virtual sanction and, by its social nature, an external sanction).

[166] In environmental law, for instance, the existence of criminal sanctions or quasi-criminal sanctions is a privileged means of demonstrating the mandatory nature of the rules imposed in particular by European directives. *See* MICHAEL G. FAURE & GÜNTHER HEINE, FINAL REPORT: CRIMINAL PENALTIES IN EU MEMBER STATES' ENVIRONMENTAL LAW 333 (2002), https://ec.europa.eu/environment/legal/crime/pdf/criminal_penalties1.pdf.

[167] Steven Shavell, *Optimal Structure of Law Enforcement* 37 J.L. & ECON. 255, 261–62 (1993).

[168] Samuel Ferey, *Histoire et méthodologie de l'analyse économique du droit contemporaine* [History and Methodology of Economic Analysis of Contemporary Law], *in* ANALYSE ÉCONOMIQUE DU DROIT [ECONOMIC ANALYSIS OF THE LAW] 11, 18–20 (B. Deffains & E. Langlais, eds., 2009). RICHARD POSNER, ECONOMIC ANALYSIS OF LAW (2014).

[169] *See* Michel van de Kerchove, *Les fonctions de la sanction pénale. Entre droit et philosophie*, 127(7) INFORMATIONS SOCIALES 22, 30 (2005)

Sanctioning has an expressive function (denunciation) because it underlines the importance that society and the public authorities give to the values and rights whose violation is sanctioned.[170] This expressive function of punishment has been highlighted by sociologists such as Emile Durkheim.[171] Society shows how precious a value is in two main ways. The law may provide for a particularly solemn procedure for the most serious crimes (special courts, intervention of popular juries, exceptional decorum, etc.).[172] The other way of emphasizing the importance of the protected value is to provide that the infringement of this right will be severely punished, either through a feared type of penalty (death penalty, imprisonment, etc.) or through a high level of punishment (number of years in prison or amount of the fine).[173] The expressive function of the sanction implies that if the society comes to recognize an important value in the protection of personal data and respect for the rights of the data subjects, then the sanctions incurred will logically be high.[174] In fact, the sanctions provided by the GDPR are indeed among the highest financial sanctions that can be applied in Europe because of the way it is

(explaining that the "socio-pedagogical" or "expressive" function of punishment may be understood as a symbolic expression of the attachment of the society to certain norms, the behaviour that conforms to them and the values that they protect).

[170] Joel Feinberg, *The Expressive Function of Punishment*, *in* WHY PUNISH? HOW MUCH? A READER ON PUNISHMENT DESERVING 111, 114 (Michael Tonry, ed., 2011).

[171] EMILE DURKHEIM, DE LA DIVISION DU TRAVAIL SOCIAL 82 [THE DIVISION OF LABOR IN SOCIETY] (1893) ("Nous ne le réprouvons pas parce qu'il est un crime, mais il est un crime parce que nous le réprouvons") [We do not condemn it because it is a crime, but it is a crime because we condemn it]. Thus, sanctions linked to the violations express the values and the collective consciousness of the society.).

[172] The most serious criminal offences are judged by special courts where particular solemnity is seen. *See* Garapon, *supra* note 124, at 54.

[173] Even in the case of international criminal law, where there are no guidelines or scale of penalties, penalties are apportioned according to the seriousness of the offenses. *See* Allison Marston Danner, *Constructing a Hierarchy of Crimes in International Criminal Law Sentencing*, 87 VA. L. REV. 415, 453 (2001) ("Tribunals have frequently stated the gravity of the offense is the most important consideration in devising a sentence").

[174] Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479, 481 (2016) ("It is important to stress at the outset that the right to privacy is a key concept in EU law and has been given significant weight that reflects deep cultural values and understandings").

calculated.[175] It should also be noted that the expressive function of the sanction does not necessarily imply that it will be actually applied. The threat of severe punishment could be enough to send a message to the public that this regulation is considered to be essential.[176] However, the sociology of delinquency also emphasizes that the application of punishment is a way for society to remind the population of the value it attributes to protected rights.[177] In this perspective, a frequent application of sanctions will tend to trivialize this set of rules and may harm the expressive function of the sanction. On the other hand, a punctual application of the sanction may be useful to affirm that society does not want to tolerate non-compliance with the law.[178] Regulatory authorities are then inclined to impose exemplary sanctions. Rather than seeking to sanction many actors, a good policy for the expressive function of a sanction will be to sanction preferably emblematic actors.[179] From this point of view, large companies that are well known to the public and the market, such as the U.S. Tech Giants, will be more exposed to the risk of sanctions than smaller and more banal companies.[180] In addition, if an actor has committed a minor regulatory violation, the GDPR allows for a reprimand instead of an

---

[175] *See, e.g.*, Nemitz, *supra* note 58, at 3 ("The GDPR in its fining system is inspired by the system of fines in European Competition Law and uses its methodology in large part. In particular, the determination of fines in terms of a percentage of overall turnover and a cap of fines determined by a set percentage of turnover of the undertaking concerned").

[176] However, the sanctions must be known to the people who incur them! *See* Robert Apel, *Sanctions, Perceptions, and Crime: Implications for Criminal Deterrence*, 29(1) J. QUANTITATIVE CRIMINOLOGY 67, 71 (2013) ("deterrence is, fundamentally, a process of information transmission intended to discourage law violation").

[177] Jack Gibbs, *Crime, Punishment, and Deterrence*, 48 SOUTHWESTERN SOC. SCI. Q. 515, 517 (1968).

[178] Non-tolerance towards delinquency, even as far as the most minor infringements are concerned, is linked to the now famous theory of the broken window. *See, generally,* G. L. KELLING & CATHERINE COLES, FIXING BROKEN WINDOWS: RESTORING ORDER AND REDUCING CRIME IN OUR COMMUNITIES (1996).

[179] *See, e.g.*, Nemitz, *supra* note 58, at 1 ("Fines serve to discourage further infringements. Art. 83 GDPR serves both special prevention and general prevention, since high fines for misconduct are attracting widespread attention, especially in the case of controllers or processors known in the market and to the general public").

[180] On the European Union's tendency to treat large digital companies more harshly, *see*, *e.g.*, Javier Espinoza & San Fleming, *EU Seeks New Powers to Penalise Tech Giants*, FIN. TIMES (Sept. 20, 2020), https://www.ft.com/content/7738fdd8-e0c3-4090-8cc9-7d4b53ff3afb.

administrative fine.[181] With regard to the expressive function of sanctions, it is the sanctions incurred that count, even if the sanctions that are actually applied may be a useful reminder. The importance of the quantum of the penalty may enhance the effectiveness of the communication achieved through sanctions. As this message complements the regulation itself, decision-making practice must be as unambiguous as the regulation itself. This argues for a decision-making practice vis-à-vis the sanctions by the different DPAs as uniform as possible.[182]

2. Normative Function

Sanctions can also play a normative function.[183] Sanctions not only help to say that a behavior is mandatory or prohibited, but also to say in useful detail what precisely is mandatory or prohibited. Sanctions decisions complement ex post the standards of behavior provided ex ante by regulation, as if there were a tacit delegation from the legislator or regulator to the judicial or regulatory authority.[184] Clarifications are all the more useful when interpreting and understanding a law based on abstract and sometimes new standards with uncertain implications.[185] The possible or effective application of a sanction for having committed a criminal offense is an indirect way of saying that the conduct in question is prohibited and that people must therefore positively avoid such conduct.[186] When sanctions are provided to ensure the effectiveness of a regulation, normative rules

---

[181] GDPR, *supra* note 1, Recital 148 ("In a case of minor infringement . . . a reprimand may be issued instead of a fine.").

[182] The search for consistency in the implementation of the GDPR is an explicit goal of the EDPB. *See Consistency Findings*, EDPB, https://edpb.europa.eu/our-work-tools/consistency-findings_en (last visited on Oct. 27, 2020).

[183] John M. Darley, Kevin M. Carlsmith & Paul H. Robinson, *The Ex Ante Function of the Criminal* Law, 35 LAW & SOC'Y REV. 165, 165–66 (2001) ("The code announces in advance what actions count as criminal; thus the citizenry can use the announcement to guide their actions to avoid criminal conduct.").

[184] MARIA JOSE FALCON Y TELLA, CASELAW IN ROMAN, ANGLOSAXON AND CONTINENTAL LAW 112 (2011).

[185] *See* Wolff, *supra* note 76, at 11.

[186] *See* Durkheim, *supra* note 171, at 77 ("Le droit pénal, tout au contraire, n'édicte que des sanctions, mais il ne dit rien des obligations auxquelles elles se rapportent. Il ne commande pas de respecter la vie d'autrui, mais de frapper de mort l'assassin. Il ne dit pas tout d'abord, comme fait le droit civil: Voici le devoir, mais, tout de suite : Voici la peine. Sans doute, si l'action est punie, c'est qu'elle est contraire » à une règle obligatoire").

are obviously included in this regulation. The principle of criminal legality normally even prevents the authority with the power to impose sanctions from punishing behavior that was not clearly and previously prohibited.[187] As far as regulatory sanctions are concerned, the principle of criminal legality is not so strict.[188]

In practice, some of the standards included in the regulations are sometimes relatively vague and case-law appears useful in clarifying the rules of behavior resulting from them. However, violations of regulations that may result in sanctions expose operators to a legal risk and a risk of sanctions that is high because the sanctions incurred are high.[189] In view of this function, it seems important that sanction decisions are actually pronounced so that the normative details are given. The authorities can accentuate this function by echoing the sanction decisions that feed into case law. In this respect, decisions may be anonymous because what matters is not the identity of the person sanctioned.[190] In contrast to the functions of sanctions that require severe penalties (such as deterrence), the amount of the sanctions is of little importance, since it is the reasoning of the decision that makes it possible to extract the information useful for the interpretation of the text. They may even be decisions concluding that the accused person has been exonerated because the explanation of the reasons why the accused was not sanctioned may very well be a source of information on the conduct that is authorized under the regulations.[191] For this normative function of sanctions to play its role properly, it is important

---

[187] Peter Westen, *Two Rules of Legality in Criminal Law*, 26(3) LAW & PHIL. 229, 305 (2007) ("the rule that criminal statutes be construed narrow").

[188] Case T-99/04, *AC Treuhand AG v. Comm'n* of the European Communities (July 8, 2008), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62004TJ0099&from=FR.

[189] It is not unusual that companies have to face legal and regulatory uncertainty. *See* P.H. Birnbaum, *The Choice of Strategic Alternatives Under Increasing Regulation in High Technology Companies*, 27(3) ACAD. MGMT. J. 489, 492–93 (1984).

[190] *See* Judges' Technology Advisory Committee (Canadian), Use of Personal Information in Judgments and Recommended Protocol, March 2005, at no. 21, https://cjc-ccm.ca/sites/default/files/documents/2019/news_pub_techissues_UseProtocol_2005_en.pdf. Luc Plamondon, Guy Lapalme & Frédéric Pelletier, Anonymisation de décisions de justice, Conference TALN 2004, at 2 http://transsearch.iro.umontreal.ca/rali/sites/default/files/publis/0UdeM-taln-04.pdf.

[191] On the merits of a dismissal decision, see, for example, the testimony of the president of a regulatory authority's sanction body: Daniel Labetoulle, *La Commission des sanctions de l'Autorité des marchés financiers: un témoignage,* 93 DROIT ET SOCIETE, 2016/2, 337, 352.

that the sanctions taken by the different DPAs are not contradictory and that they complement each other. Also, with regard to this function, the uniform application of sanctions must prevail in the European regulatory style.[192]

D. Deterrence and Incapacitation

In terms of regulatory sanctions, the function that often appears to be the most important is the deterrence function (Section 1). The sanction serves primarily to prevent individuals or companies from committing infringements in the future. The financial loss that the offender could suffer in case of sanction is anticipated and taken into account in his or her economic calculation, so that the violation appears to him or her to be economically inopportune. Then we will see that sanctions can also help to prevent the commission of offenses by impacting not only the anticipations of potential offenders but also on their means of committing the offenses. In classical criminal law, this refers to the function of incapacitation (Section 2).

1. Deterrence

From the deterrence perspective, the sanction must be sufficiently severe in order to play its disciplinary role.[193] The right sanction is the one that is sufficiently dissuasive to encourage operators to comply strictly with the rules determining how to behave. Paradoxically, the effectiveness of the sanctions then lies in its ability not to be applied.[194] The economic theory of crime developed from Gary Becker's seminal article,[195] following the pioneering work of Jeremy Bentham,[196] specifies the conditions under which a sanction can be deterrent. Assuming that the agents are rational, a sanction will be dissuasive if the anticipated sanction (taking into account the probability that the offense will be detected, prosecuted and effectively

---

[192] Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 430 (2011).
[193] *See, e.g.*, Nemitz, *supra* note 58, at 1.
[194] *See*, *e.g.*, Steven Shavell, *Criminal Law and the Optimal Use of Nonmonetary Sanctions as a Deterrent*, 85 COLUM. L. REV. 1232 (1985).
[195] Gary G. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POLITICAL ECON. 169 (1968).
[196] JEREMY BENTHAM, AN INTRODUCTION TO PRINCIPLES OF MORALS AND LEGISLATIONS, in THE WORKS OF JEREMY BENTHAM 396 (J. Bowring, ed., 1838) (1789).

sanctioned)[197] is greater than the anticipated benefit in the case of a violation of the norm belonging to the criminal law. The economic analysis of crime also underlines that the deterrent effectiveness of the sanction will vary according to the risk aversion of the agents. According to Becker, agents with high risk aversion are deterred more by severe penalties than by an increase in the probability of detection.[198] Conversely, if they are less risk-adverse, the increase in the probability of detection will be more effective.[199] According to Beccaria, the certainty and swiftness of the sentence is more important than its intrinsic severity.[200]

The GDPR changes both parameters, however. On the one hand, the penalties incurred are significantly increased; on the other hand, thanks to the specialization of specific regulatory authorities in the field of personal data protection with a supervisory role for companies in this industry, and significant and harmonized investigation powers (the DPAs), the probability of detecting regulatory violations is increased.[201] In addition, the fact that the rules and sanctions are common to all EU Member States and that the DPAs can jointly exercise the power of sanction reduces the likelihood that companies will escape them by exploiting the diversity of regulations and the lack of coordination between regulatory authorities.[202]

---

[197] In another field, *see* Steven Klepper & Daniel Nagin, *Tax Compliance and Perceptions of the Risk of Detection and Criminal Prosecution*, 23 L. & SOC'Y REV. 209 (1989) (stating that in another field, S. Klepper and D. Nagin emphasize the empirical importance of the perception of detection risk within a particular social group such as that of administrators on the deterrent effect of the sanction and on the fear of criminal prosecution).

[198] Bruno Deffains, *Existe-t-il de bonnes sanctions d'un point de vue économiques? [Are There Good Sanctions from an Economic Point of View?]*, *in* LES SANCTIONS DES SOCIETES COTEES [SANCTIONS OF LISTED COMPANIES] 53, 75 (Arnaud Reygrobellet & Nathalie Huet, eds., 2012).

[199] *See* Mitchel A. Polinsky & Steven Shavell, *The Optimal Trade-Off Between the Probability and Magnitude of Fines*, 69 AM. ECON. REV. 880, 880 (1979); *see also* Lucian A. Bebchuk & Louis Kaplow, *Optimal Sanctions and Differences in Individuals' Likelihood of Avoiding Detection*, 13 INT'L REV. L. & ECON. 217, 223 (1993); *see also* Nuno Garoupa, *Optimal Magnitude and Probability of Fines*, 45 EUR. ECON. REV. 1765, 1765 (2001); *see also* Jeffrey Grogger, *Certainty vs. Severity of Punishment*, 29 ECON. INQUIRY 297, 297 (1991).

[200] CESARE BECCARIA, DEI DELITTI E DELLE PENE [ON CRIME AND PUNISHMENT] chs. 19 & 41 (1764).

[201] GDPR, *supra* note 1, art. 58.

[202] Hugues Bouthinon-Dumas, *Economic Analysis of the Interaction Between National Legal Systems: A Contribution to the Understanding of Legal*

In the field of deterrence, it is the penalties incurred that count *a priori* more than the penalties actually imposed.[203] Ideally, the mere potentiality of imposing sanctions is sufficient to persuade those who might be tempted by the transgression to give up this temptation. But if transgressions do occur, the fact that they are not sanctioned or not sanctioned severely enough destroys the credibility of the threat. If non-compliance, including serious non-compliance, can be observed, the proper functioning of deterrence requires that sanctions be effectively imposed and that they be sufficiently severe to update the deterrent effect, especially because the possibility of a sanction actually being applied tends to be underestimated by actors as it is a contingent future event.[204] This attitude must be adopted by the different authorities, and it is therefore again recommended that there should be a uniform sanctions policy.

2. Incapacitation

Sanctions can also reduce the chances that violations of the law will occur by acting on the potential perpetrators and their means of action beyond their expectations.[205] Regulators may also be tempted to impose the very high financial penalties at that may weaken or even exclude from the market an operator who has violated data protection regulation.[206] This corresponds to the incapacitation function of the sanction, which is a means of protecting society and the market against

Diversity and Legal Unity, 11 J. CIV. L. STUD. 320 (2018) ("Certain forms of harmonization such as the establishment of social and economic standards (e.g., minimal wages, maximum working time) are other ways of overseeing competition between national systems. In other words, regulatory competition should be mitigated and circumscribed through state cooperation").

[203] IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION 6 (1992).

[204] Bottoms & Von Hirsch, *supra* note 105, at 106.

[205] FRANKLIN E. ZIMRING & GORDON HAWKINS, INCAPACITATION: PENAL CONFINEMENT AND THE RESTRAINT OF CRIME (1995); Bottoms & Von Hirsch, *supra* note 105, at 113 ("Whereas rehabilitation and special deterrence seek to affect offenders' choices so they refrain from committing crimes, incapacitation requires no such change").

[206] *See*, *e.g.*, Curtis Poe, *Is GDPR the New Way to Bankrupt Companies?*, QUORA (Nov. 28, 2018), https://www.quora.com/Is-GDPR-the-new-way-to-bankrupt-companies (the author of this blog response, who identifies himself as the CTO of https://allaroundtheworld.fr/, states "the GDPR was created with the specific intention of levying incredibly punitive fines against companies for not taking this seriously. And yes, that means driving companies into bankruptcy for the worst violators of consumer rights").

the risk that the sanctioned entity will repeat its harmful behavior.[207] The way in which the maximum financial penalties is determined, based on a high absolute value for small and medium-sized companies and even more so as a multiple of turnover, makes it possible to fine almost all companies very heavily.[208] This method of calculation is potentially more severe than calculating sanctions on the basis of profits or benefits from a reprehensible practice. It makes it possible to fine companies that, in the cycle of their development, already have consequential economic activity but are not yet profitable and, therefore, do not yet generate a profit.

Incapacitation is a traditional objective of criminal law enforcement.[209] It involves either removing the offender from society (by imprisonment) or from a particular activity (by banning him from practicing), or applying a specific sanction aimed at acting on the roots of his offending behavior. This concern is not necessarily unrelated to the policy of applying financial sanctions to entities that violate the GDPR. Admittedly, there are measures other than financial sanctions that are more directly relevant for ensuring that regulated entities are in compliance, such as injunctions relating to the obligation to set up an internal compliance program, as a form of probation for companies.[210] But financial sanctions can indirectly play a role in this perspective. Indeed, a heavy financial penalty will often have the effect of bringing about a major change within the company—the company's strategy and internal organization may be radically reformed following the sanction, even if this transformation is not the subject of an explicit injunction from the regulator. It is also not infrequent for the company's top management to be removed and replaced by new executives to implement the reformed strategy and incorporate the compliance requirement lacking. This incentive for the company to reform will be stronger if the sanctions are more severe. The most severe financial

---

[207] W. Robert Thomas, *Incapacitating Criminal Corporations*, 72 VAND. L. REV. 905 (2019).

[208] *See infra* Part II.C.1. (discussing "wealth-based punishment").

[209] The main application of sentencing theory as a means of preventing crime (and not just deterring it) concerns pre-trial detention and long prison sentences or even life sentences, or even the death penalty. *See, e.g.*, Thomas J. Miceli, *Deterrence and Incapacitation Models of Criminal Punishment: Can the Twain Meet?, in* RESEARCH HANDBOOK ON THE ECONOMICS OF CRIMINAL LAW 122, 122–23 (2012) ("Another explanation is that prison serves an incapacitation function; that is, it allows the state to detain those offenders who are expected to commit further harmful acts if released.").

[210] William S. Lofquist, *Legislating Organizational Probation: State Capacity, Business Power, and Corporate Crime Control*, 27 LAW. & SOC'Y REV. 741, 742 (1993).

sanctions may also result in the company being weakened to the point of bankruptcy or having to be absorbed by another company. In such cases, the most severe sanctions (in relation to the economic strength of the firm) will result in the market foreclosure of the non-compliant entity.[211] The considerable amounts of penalties incurred in relation to personal data make it possible to imagine such a hypothesis. As the sanction has a very strong impact on competition, it is essential that the policy for the application of the GDPR is uniform, so as not to contribute to introducing distortions of competition between the sanctioned undertakings and those that might escape sanctions without this protection being deserved.[212] This requirement is particularly based in EU law on the principle of equal treatment.[213]

E. Conclusion on the Goals of Sanctions

In view of the objective of preventing infringements of the GDPR, we note that regulatory sanctions should be imposed whenever justified, they should be as severe as necessary and they should be applied in a uniform manner regardless of the jurisdiction where the proceedings may be initiated.[214]

---

[211] The anticipation that a very high fine could lead to the weakening or even bankruptcy of a company is taken into account in competition law. In competition law, the disappearance of a competitor is rather analyzed as a perverse effect of a too severe sanction policy. Outside of competition law, the provoked disappearance of a delinquent firm does not pose the same problem. *See* Lianos, *supra* note 92, at 37 ("excessive fines may lead to the insolvency of the undertakings to which they have been imposed. This might not necessarily be a problem, as the risk of insolvency following the imposition of a fine may have potential deterrence effects. Yet, it may also lead to negative welfare effects, if it excludes one of the very few competitors in a market characterized by barriers to entry.").

[212] Uniform application of the sanction policy with respect to companies operating in the same market is a condition of fairness among competitors. *See* Macrory, *supra* note 93, at 231 ("One of the prime goals of a sanctioning system should be to ensure that no financial gain or benefit is made from non-compliance, and any economic gains recovered. This is only fair to competitors who comply with regulatory requirements.").

[213] *See* Nemitz, *supra* note 58, at 6 ("The supervisory authorities must comply with the general principles of law of the European Union and the law of the Member States, in particular the principle of equal treatment. As a result, DPAs have a duty to develop an administrative practice for imposing fines in order to deal with similar cases in a similar way.").

[214] *See* Yoram Shachar, *Sentencing as Art*, 25 ISR. L. REV. 638, 653 (1991) (for a discussion about the multiplicity of purposes and the need for effective sentences).

Finally, an analysis of the different goals assigned to the sanctions that DPAs are likely to impose leads to the conclusion that the predominant purpose of these sanctions is to make effective the legal and regulatory framework that DPAs are responsible for enforcing. In this respect, perhaps the most important sub-goal is deterrence in the broadest sense of the term, which consists in threatening regulated entities with sanctions that are sufficiently severe to convince them to not be tempted by non-compliance. We have observed, however, that the sub-goals that financial sanctions are likely to serve are more diverse. As may be deduced from the above, symbolic sanctions do not necessarily require heavy sanctions to be imposed, but they still require that sanctions are actually applied when there is a transgression to remind, clarify and update the message to market participants. As sanctions often have a material dimension, heavy sanctions appear to be necessary with regard to powerful players and to punish the most significant misconduct. Finally, uniform application is recommended so that most of the functions of sanctions can be fulfilled.[215] Now, this study turns to the specific sanctions provided under the GDPR, both in the text of the law and in practice.

II. GDPR SANCTIONS

No sooner had the GDPR become applicable than the first actions under it were brought by digital rights groups in Europe: among them, those by NOYB.eu (None of Your Business, or NOYB), a group created by the Austrian activist Maximilian Schrems,[216] and others by the French organization La Quadrature du Net (LQDN).[217] However,

---

[215] *See*, *e.g.*, Nemitz, *supra* note 58, at 5 ("With the entry into force of the Regulation, data protection authorities must be prepared to sanction infringements of the Regulation as consistently as possible under the Regulation, and in order to obtain a strong deterrent against non-compliance.").

[216] See Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 427–29 (2019). *See also* Henry Farrell & Abraham Newman, *Here's How Europe's Data Privacy Law Could Take Down Facebook*, WASH. POST (May 25, 2018, 7:03 AM), https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/heres-how-europes-gdpr-may-take-down-facebook/.

[217] *See* Nicholas Vinocur, *'We Have a Huge Problem': European Tech Regulator Despairs Over Lack of Enforcement*, POLITICO (Dec. 27, 2019, 5:04 AM), https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605 ("Another long-waiting party is La Quadrature du Net, a French digital rights group that filed no fewer than seven lawsuits against five big tech companies just a few days after GDPR came online.").

sanctions were already provided for under the EU DP Directive.[218] What is new includes: additional obligations under the GDPR; [219] the extent of potential administrative sanctions;[220] and the powers of the DPAs.[221]The GDPR provides for various legal actions for data protection violations and for sanctions.[222]

This section begins with a discussion of sanctions and other actions under the EU DP Directive, then continues with an enumeration of the kinds of actions and sanctions possible under the GDPR.

A. Sanctions and Other Actions Under the EU DP Directive

The EU DP Directive provided that Member States should establish sanctions for infringement of its terms: "The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."[223] It is thus clear that a crucial role of sanctions that regulatory authorities may impose is to ensure the effectiveness of a legal framework.[224] However, as the EU DP Directive was a directive and not a regulation, Member States had significant discretion regarding the form and method of its implementation in national law.[225] This extends to the establishment of sanctions and the setting of their amounts, as illustrated, for example, by the contrast between the UK law and that of France: the UK law was only amended to give its supervisory authority (data protection agency, or "DPA") the power to issue sanctions in 2010,[226] and then set the maximum penalty at £500,000,[227] a figure that was higher than the €150,000 maximum established for the French DPA, which was

---

[218] EU DP Directive, *supra* note 4, art. 24.
[219] *See* Houser & Voss, *supra* note 15, at [71]–[95].
[220] *See id.* at [57].
[221] GDPR, *supra* note 1, art. 58.
[222] *Id.* arts. 77–84.
[223] *Id*.
[224] *See*, *e.g.*, Neil Gunningham, *Enforcement and Compliance Strategies*, *in* THE OXFORD HANDBOOK OF REGULATION 120 (R. Baldwin et al., eds., 2010) ("Effective enforcement is vital to the successful implementation of social legislation, and legislation that is not enforced rarely fulfills its social objectives.").
[225] *See* W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17(9) J. INTERNET L. 1, 13 (Mar. 2014).
[226] *See* Grant & Crowther, *supra* note 8, at 288.
[227] *Id*. at 289.

empowered to issue sanctions by a 2004 amendment to its data protection act.[228] Thus, under the EU DP sanctions were not uniform among the various Member States and their DPAs,[229] whereas harmonized sanctioning practices is a condition for achieving the goals of sanctions.[230]

DPAs were given investigative powers, powers of intervention (such as ordering a ban on processing, or ordering the erasure or destruction of data), and the power to engage in legal proceedings for violation of national implementing legislation.[231] Furthermore, judicial remedies for data protection were afforded to persons for breaches of their rights,[232] and they could seek compensation for damage resulting from unlawful processing or acts otherwise incompatible with data protection law.[233] However, there was aa divergence among the Member State DPAs, with those of certain nations—for example, Germany and Spain—being tough regulators, while those of other Member States, such as Ireland and the United Kingdom, were seen as

---

[228] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law No. 2004–801 of Aug. 6, 2004 Relating to the Protection of Individuals with Regard to the Processing of Personal Data and Amending Law No. 78–17 of Jan. 6, 1978 on Information Technology, Data Files and Civil Liberties], J.O. du 6 aou. 2004, p. 14063.FRANCE

[229] *See* Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2(3) EUR. DATA PROTECT. L. REV. 287, 288 (referring the situation before the GDPR as one "where 28 different legal systems as well as 28 different judicial and enforcement cultures define the regulatory environment"), https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf. *See also* Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What it is and What it Means*, 28(1) INFO. & COMM. TECH. L. 65, 93 (2019) (referring to the EU DP Directive, the authors state that "the Directive left fines and other remedies to individual member states. Some countries implemented the Directive with maximum fines of a couple of thousand euros – so low to be completely inconsequential to many businesses."),
https://www.tandfonline.com/doi/pdf/10.1080/13600834.2019.1573501.

[230] This is true, for example, regarding the incapacitation function of sanctions, so as not to distort competition between sanctioned undertakings. *See supra* Part I.D.2. This is also true with respect to the retributive and rehabilitative role of GDPR sanctions. *See supra* Part I.A.2. Furthermore, such harmonization of sanctions is desirable for the remedial function. *See supra* Part I.B.3.

[231] EU DP Directive, *supra* note 4, art. 28(3).

[232] *Id*. art. 22.

[233] *Id*. art. 23(1).

more accommodating to business.[234] Enforcement powers of DPAs varied as well depending on applicable law and the individual DPA's strategy; although, there was hope that in the European Union, at least, the GDPR would harmonize powers.[235] Obligations were almost exclusively placed on the data controller,[236] and this fact has been seen as a weakness under national implementing legislation.[237]

In addition, the publicity created by certain DPAs with respect to fines issued may be seen as a deterrent in and of itself, perhaps being at least as important as the actual fines for multinational companies, as it could be potentially damaging for the company's reputation in the eyes of its customers and the public, as we have noticed.[238] Moreover, the amounts of the fines themselves may have been too low to deter such companies under the EU DP Directive.[239] However, overall fines play a role in awareness-raising and in allowing for there to be a "business case" for data protection compliance.[240] Thus, the denunciation function and the normative function could be performed by the fines under the Directive.

B. Kinds of Actions and Sanctions Possible Under the GDPR

Since the adoption of the GDPR much attention has centered on administrative sanctions issued by the Member State national data

---

[234] *See*, *e.g.*, WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 269 (2016) ("Germany and Spain are generally considered more stringent regulators than the UK or Ireland, for example.").

[235] *See* David Wright, *Enforcing Privacy*, in ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 13, 23–24 (David Wright & Paul De Hert eds., 2016).

[236] EU DP Directive, *supra* note 4, art. 2(d). Various articles provide for the controller to be responsible for compliance with data protection requirements. *See*, *e.g.*, *id*. art. 6(2) (providing that controllers are to ensure compliance with data quality principle requirements); *Id*. arts. 10–11 (providing that in Member States, the controller or his representative shall provide the data subject with information regarding the collection of his data); *Id*. art. 17 (providing that Member States shall require the controller to implement measures to ensure the security of data, and be responsible for vetting, with respect to guarantees in respect of security, any processor who processes data on the controller's behalf).

[237] *See*, *e.g.*, GRAHAM J.H. SMITH, INTERNET LAW AND REGULATION (4th ed. 2007) 716–17, ("The [Information] Commissioner may not serve enforcement notices on data processors and others: this is a weakness in the [Data Protection Act of 1998].") (regarding the UK DPA and implementing legislation).

[238] *See* Grant & Crowther, *supra* note 8, at 299.

[239] *Id*. at 301.

[240] *Id*. at 304.

protection agencies for EU data protection law violations.[241] However, that is only one of the tools of the data protection enforcement toolbox: individuals who are harmed may (1) lodge a complaint with a supervisory authority,[242] (2) bring an action for effective judicial remedy against a supervisory authority before the courts of Member State where the supervisory authority is established,[243] (3) individually seek to obtain a judicial remedy against a controller or a processor in an appropriate jurisdiction,[244] or (4) mandate a non-profit public-interest consumer or digital rights organization to lodge a complaint on his or her behalf, either with a supervisory authority or a court.[245] Each of these options is discussed below. Note that, in addition to these options, Member States may specify additional penalties for infringements which are not subject to administrative fines;[246] although, those penalties, to the extent they exist, are beyond the scope of this study, which is focused on sanctions actually provided in the GDPR.

1. Actions Before (or by) the Relevant Supervisory Authority and Its Possible Range of Sanctions

Data subjects have the right to file a complaint with a supervisory authority for an alleged infringement of data protection law involving their personal data.[247] They may choose the supervisory authority of their habitual residence, workplace, or place of alleged

---

[241] *See*, *e.g.*, Olivia Tambou, *Lessons From the First Post-GDPR Fines of the CNIL Against Google LLC*, 5 EUR. DATA PROT. L. REV. 80 (2019) (discussing how the CNIL's administrative sanction issued to Google "got a great deal of media attention as well as in the community of 'digital actors'."). *See also* Houser & Voss, *supra* note 15, at [3] (highlighting the increased administrative sanctions under the GDPR, "potentially increasing maximum fines to over $1 billion for a company such as Facebook and over $3 billion for one such as Google."); and *see* Hoofnagle et al., *supra* note 229, at 93 (speaking to changes to EU data protection as a result of the adoption of the GDPR, the authors refer to administrative sanctions and state, "changes with respect to sanctions are the most spectacular.").

[242] GDPR, *supra* note 1, art. 77.

[243] *Id.* art. 78.

[244] *Id.* art. 79.

[245] *Id.* art. 80.

[246] *Id.* art. 84 (discussing that these penalties may be criminal penalties). *See also* GDPR, *supra* note 1, Recital 149 ("Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation."). The references to criminal penalties in Part I of this study will be relevant for the reader interested in criminal penalties.

[247] *Id.* art. 77(1).

infringement.[248] The relevant supervisory authority must inform the complainant about the possibility of a judicial remedy, and the progress and outcome of the complaint.[249]

With respect to controllers or processors, the Supervisory Authority has the power to: issue warnings where processing operations are likely to infringe the GDPR;[250] issue reprimands where processing operations have infringed the GDPR;[251] and order compliance with requests to exercise data subject rights;[252] to order the bringing into compliance of processing operations with the GDPR (including within a specified manner or period, if appropriate).[253] In addition, it may order a controller to make a data breach notification to a data subject.[254] Furthermore, it may order a temporary or definitive

---

[248] GDPR, *supra* note 1, art. 77(1).
[249] *Id.* art. 77(2).
[250] *Id.* art. 58(2)(a); *see* European Data Protection Board (EDPB), Contribution of the EDPB to the evaluation of the GDPR under Article 97 (2020), 1, 32. (stating that the following fourteen countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Cyprus, Czech Republic, Germany, Estonia, France, Greece, Hungary, Italy, Lithuania, Latvia, Malta and the United Kingdom) [hereinafter EDPB].
[251] GDPR, *supra* note 1, art. 58(2)(b); *see* EDPB, *supra* note 250, at 32 (stating that the following twenty-four countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Germany, Denmark, Estonia, Spain, Finland, France, Greece, Hungary, Italy, Lithuania, Latvia, Malta, the Netherlands, Norway, Poland, Romania, Sweden, Slovakia and the United Kingdom).
[252] GDPR, *supra* note 1, art. 58(2)(c); s*ee* EDPB, *supra* note 250, at 32 (stating that the following twenty-five countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Germany, Denmark, Estonia, Spain, Finland, France, Croatia, Hungary, Iceland, Italy, Lithuania, Latvia, Malta, Norway, Poland, Portugal, Romania, Sweden, Slovenia and Slovakia).
[253] GDPR, *supra* note 1, art. 58(2)(d); *see* EDPB, *supra* note 250, at 33 (stating that the following twenty-seven countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Germany, Denmark, Estonia, Spain, Finland, France, Greece, Croatia, Hungary, Iceland, Italy, Lithuania, Latvia, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Sweden, Slovenia and Slovakia).
[254] GDPR, *supra* note 1, art. 58(2)(e); *see* EDPB, *supra* note 250, at 33 (stating that the following ten countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Denmark, Finland, France, Hungary, Iceland, Italy, Malta, Poland and Latvia).

ban on processing,[255] the correction or erasure of personal data,[256] the withdrawal of a data protection certification,[257] or the suspension of cross-border data flows.[258] Moreover, and perhaps most importantly for the purposes of this study, a Supervisory Authority may impose administrative fines either in place of, or in addition to, other measures mentioned in this paragraph.[259] The amount of these administrative fines is discussed in Section C.1. Administrative sanctions (other than administrative fines) help to deter market participants from breaking the rules and damaging the interests of data subjects. The deterrent power of these administrative measures, on the one hand, and administrative fines, on the other hand, is cumulative.[260] The graduated response policy advocated by the GDPR is probably more relevant than a policy of sanctions, which would have at its disposal only the weapon of a formidable sanction.

---

[255] GDPR, *supra* note 1, art. 58(2)(f); *see* EDPB, *supra* note 250, at 33 (stating that the following thirteen countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Germany, Denmark, Greece, Hungary, Iceland, Italy, Lithuania, Malta, the Netherlands, Portugal, Romania and Slovenia).

[256] GDPR, *supra* note 1, art. 58(2)(g); *see* EDPB *supra* note 250, at 33 (stating that the following seventeen countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Spain, Finland, Croatia, Hungary, Iceland, Luxembourg, Latvia, Norway, Poland and Portugal).

[257] GDPR, *supra* note 1, art. 58(2)(h); *see* EDPB, *supra* note 250, at 33 (stating that no country used this power during the period from May 25, 2018 to November 30, 2019).

[258] GDPR, *supra* note 1, art. 58(2)(j); *see* EDPB, *supra* note 250, at 33 (stating that no country used this power during the period from May 25, 2018 to November 30, 2019).

[259] GDPR, *supra* note 1, art. 58(2)(i); *see* EDPB, *supra* note 250, at 33 (stating that the following twenty-two countries used this power during the period from May 25, 2018 to November 30, 2019: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Germany, Denmark ("the legal system of Denmark does not allow for administrative fines. Fines can only be imposed by the national courts, which means that the Danish SA reports infringements to the Police, which then takes the case to court"), Spain, France, Greece, Hungary, Italy, Lithuania, Latvia, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Sweden and Slovakia).

[260] GDPR, *supra* note 1, art. 83(2) ("Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2).").

2. Actions Against the Supervisory Authority

Proceedings against supervisory authorities may be brought before EU Member State courts where such authorities are established,[261] and they may concern the attempt to obtain an effective remedy: (i) against a legally-binding decision concerning the complainant,[262] (ii) where the supervisory authority does not handle a complaint or inform the complainant within three months of the outcome or progress of it.[263] The possibility for market participants to take legal action against supervisory authorities, and for courts to hear such cases, is required for an effective judicial remedy and is consistent with the Additional Protocol to the Council of Europe's Convention 108, and to the modernized version of that Convention.[264]

In addition to having the possibility of lodging a complaint with a supervisory authority, a data subject may also seek effective relief against a controller or processor in the courts (the actions are without prejudice to one another).[265] This would be the case where the data subject considers that his or her rights under the GDPR have been infringed by non-compliant processing of his or her personal data.[266] There are alternative possible jurisdictions for the case: the courts of the EU Member State, (i) where the controller or the processor, as the case may be, has an establishment, or (ii) of the data subject's habitual residence, unless the defendant is "a public authority of a Member State acting in the exercise of its public powers."[267] If a competent court of an EU Member State knows of proceedings on the same matter involving data processing by the same controller or processor, as the case may be, it contacts the other court to confirm the existence of such proceedings,[268] and any court other than the one where the case is first brought may suspend proceedings.[269] In a similar manner, any court other than the one where the case is first brought may decline

[261] *Id*. art. 78(3).
[262] *Id.* art. 78(1).
[263] *Id.* art. 78(2).
[264] *See* Waltraut Kotschy, *Article 78. Right to an Effective Judicial Remedy Against a Supervisory Authority, in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1125, 1127–28 (Christopher Kuner et al., 2020).
[265] GDPR, *supra* note 1, art. 79(1).
[266] *Id.*
[267] *Id.* art. 79(2).
[268] *Id.* art. 81(1).
[269] GDPR, *supra* note 1, art. 81(2).

jurisdiction upon application of one of the parties, if the first court has jurisdiction and its law permits consolidation of the claims.[270]

The claimant, who may be the data subject or another injured party,[271] has the right to compensation from the controller or the processor, as the case may be, if he or she has suffered damage (whether material or non-material) because of infringement of the GDPR.[272] Such damage may be financial, physical or psychological.[273] Controllers are liable for damage caused by processing that infringes the GDPR, if they are involved in processing. Processors, on the other hand, are only liable for damage related to non-compliance of obligations specifically addressed to processors in the GDPR, or where they have acted against the relevant controller's lawful instructions.[274] In both cases, there may be an exemption from liability if the controller or processor, as the case may be, proves that "it is not in any way responsible for the event giving rise to the damage."[275] Where there are joint controllers or processors or both controller and processor are involved in the processing that causes the damage, each shall be held liable for the entire damage[276] and the one who pays the full compensation is entitled to claim back a share (based on their relative parts of responsibility) from the other controller or processor involved in the proceeding.[277] As a result of this potential for joint liability, processing agreements, whether in the context of joint controllers or the more traditional relationship between a controller and a processor, should clearly set out the responsibilities of each party, as indicated by Articles 26 and 28 of the GDPR, and this should include responsibilities for eventual claims.[278] However, France, for one, has added the possibility of class action law suits for data protection

---

[270] *Id.* art. 81(3).

[271] *See* Heledd Lloyd-James & Peter Carey, *The Rights of Individuals*, in DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 122, 152 (Peter Carey, ed., 5th ed., 2018) ("It is not necessary for the claimant to be the data subject in relation to the relevant processing.").

[272] GDPR, *supra* note 1, art. 82(1).

[273] *See* Lloyd-James & Carey, *supra* note 271, at 152 ("Claims for compensation may be brought for financial, physical, and psychological damage as well as for distress caused by an infringement of the GDPR.").

[274] GDPR, *supra* note 1, art. 82(2).

[275] *Id.* art. 82(3).

[276] *Id.* art. 82(4).

[277] *Id.* art. 82(5).

[278] *See* Lloyd-James & Carey, *supra* note 271, at 151–52.

violations,[279] and the GDPR has included actions by non-profit organizations mandated by individuals, as this study will now discuss. In the case of the GDPR, such measure is intended to make easier and enhance the defense of data subject interests,[280] thus facilitating reparation. This is useful since we noted that the reparation function was not directly fulfilled by administrative fines.

3. Actions by Non-Profit Organizations Mandated by Individuals

Procedural rules relating to private enforcement certainly have a potential effect on the effectiveness of regulation: the easier it is to initiate legal proceedings and the more open they are to a large number of potential claimants, including activist NGOs, the more likely it is that regulations and rights will be respected.[281] Concern for effective regulation would be served not only by financial penalties as a deterrent to transgressing the applicable standards, but also by private enforcement actions.

Under the GDPR, a data subject may mandate a non-for-profit body, organization or association, properly organized under the law of an EU Member State, whose purpose is in the public interest, and that is active in protection of data subject rights and freedoms regarding the processing of their personal data, to file a complaint, to apply to a court for relief against a supervisory authority, or to seek an effective remedy against a controller or processor on its behalf.[282] Furthermore, EU Member States may grant to such bodies, organizations or associations to take such actions independent of any mandate, if it considers that data subject rights under the GDPR have been infringed.[283] While the European Commission acknowledges that several actions were started by NGOs mandated by individuals, it commented that "recourse to representative actions would have been easier if more Member States had made use of the possibility provided for by the Regulation to allow non-governmental organisations to launch actions without a

---

[279] Loi 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle [Law No. 2016-1547 of Nov. 18, 2016 to Modernize XXIst Century Justice], J.O. du 19 nov. 2016, p. 269.

[280] *See* Gloria González Fuster, *Article 80. Representation of Data Subjects*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1142, 1143 (Christopher Kuner et al., 2020).

[281] *See*, *e.g.*, Federica Casarosa, *Transnational Collective Actions for Cross-Border Data Protection Violations*, 9(3) INTERNET POL'Y REV. 1, 3 (2020) https://www.econstor.eu/bitstream/10419/224938/1/1733852298.pdf.

[282] GDPR, *supra* note 1, art. 80(1).

[283] *Id.* art. 80(2).

mandate."[284] Since private enforcement techniques are available in different ways in the EU Member States, it appears that deterrence through administrative fines remains the minimum basic mechanism to ensure effective regulation. Private enforcement appears to be a complementary, and not a generalized mechanism.

However, the Commission has proposed a new Directive on representative actions for the protection of the collective interests of consumers,[285] which is intended to apply to data protection, among other areas.[286] This proposed Directive is in the legislative process and, on March 26, 2019, an amended version of the proposed Directive was approved by the Parliament on first reading, but, as of July 30, 2020, the legislative text still awaits the Council's first reading position.[287] The proposed Directive, if adopted in the form proposed by the Commission, would enable "qualified entities to seek representative actions aimed at the protection of consumers, while ensuring appropriate safeguards to avoid abusive litigation."[288] It would also allow for redress measures, including those for compensation,[289] and EU Member States would be able to provide, alternatively, for courts or administrative authorities to issue declaratory decisions with respect to listed EU legislation "regarding the liability of the trader toward the consumers harmed by an infringement . . . in duly justified cases where, due to the characteristics of individual harm to the consumers concerned the quantification of individual redress is complex,"[290] with

---

[284] *Communication from Commission to the European Parliament and the Council, Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock*, at 7, COM (2019) 374 final (July 24, 2019).

[285] *Proposal for a Directive of the European Parliament and of the Council on Representative Actions for the Protection of the Collective Interests of Consumers, and Repealing Directive,* COM (2018) 184 final (Apr. 11, 2018).

[286] *Id.* recital (6) at 19; *see Annexes to the Proposal for a Directive of the European Parliament and of the Council on Representative Actions for the Protection of the Collective Interest of Consumers, and Repealing Directive 2009/22/EC*, at 5, COM (2018) 184 final (Apr. 11, 2018), (illustrating the GDPR figures on the list of EU legislation to be covered by the proposed Directive).

[287] *See* Representative Actions for the Protection of the Collective Interests of Consumers, PARL. EUR. DOC. (COD 0089) (2018), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0089(COD)&l=en (last visited on July 30, 2020).

[288] *Proposal for a Directive*, *supra* note 285, art. 1(1) at 26.

[289] *Id*. art. 6(1) at 28.

[290] *Id*. art. 6(2) at 28; *see Internet, New Technologies, and Value, supra* note 14, at 482–84 (explaining that the quantification of redress for personal data is famously complex, as there is a lack of transparency on the part of the U.S.

certain exceptions.[291] Importantly, the proposed Directive provides for cross-border representative actions:

> Member States shall ensure that where the infringement affects or is likely to affect consumers from different Member States the representative action may be brought to the competent court or administrative authority of a Member State by several qualified entities from different Member States, acting jointly or represented by a single qualified entity, for the protection of the collective interest of consumers from different Member States.[292]

This move toward collective redress (CR) is part of an evolution of EU law from a focus on institutions or individuals taking action to collective action, which has specifically been called for in the areas of "consumer protection, competition, environment protection, protection of personal data, financial services legislation and investor protection."[293]

Having presented the sanctions other than the administrative fines, it appears that the competition between types of sanctions or legal actions does not undermine the specific effectiveness of administrative sanctions in terms of the objectives we have listed. On the contrary, the different types of sanctions complement each other, either because administrative fines do not achieve certain goals (*e.g.*, reparation for victims) or because other sanctions actually increase the effectiveness of administrative fines (*e.g.*, the regulator's injunctions which both precede and are secured by the fines).

C. The Quantum of Administrative Sanctions

The quantum of administrative sanctions imposed on violators of data protection law is the subject of this Section, as well as the subject of many commentators on the GDPR. This study will start this

---

Tech. Giants regarding their value, and there is also a "collective effect of cumulated data," making them more valuable collectively than cumulatively. This all argues for collective redress).

[291] *Proposal for a Directive*, *supra* note 285, art. 6(3) at 28–29.

[292] *Id*. art. 16(2) at 32.

[293] Sara Benedi Lahuerta, *Enforcing EU Equality Law Through Collective Redress: Lagging Behind?*, 55 COMMON MKT. L. REV. 783, 792 (2018) ("EU law has, therefore, evolved from its initial focus on institutional and individual vigilance to recognize, more recently, that collective vigilance, particularly CR and broader standing rules, are necessary to make the enforcement toolkit more comprehensive and effective.") (citation omitted).

subject by detailing the relevant text of the GDPR and its development (Section 1), then will explain the "one-stop-shop" mechanism (Section 2), before comparing sanctions prior to the GDPR to those after its application date (Section 2).

1. The Text of the GDPR and Its Development

The text of the GDPR was developed over a period that began well before the eventual application of the legislation in May 2018. In the European Commission's initial proposal of the GDPR, which was released on January 25, 2012, a proposed Article 79 aimed to empower DPAs to impose administrative sanctions that were to be "in each individual case effective, proportionate and dissuasive."[294] This language regarding sanctions was retained in the final version of the GDPR.[295] The goal was to be achieved in the context of what was to be strong enforcement of the data protection rules.[296] Implementation was expected to lead to, in the Commission's analysis, "consistency of data protection enforcement in the Union, the effective possibility of individuals to exercise their data protection rights to the protection of personal data within the EU and the efficiency of data protection supervision and enforcement."[297]

The initial Commission proposal for the GDPR gave DPAs the power to sanction administrative offenses,[298] and provided that administrative sanctions should go on a sliding scale, from mere warnings, to a first level of €250,000 or 0.5% of annual worldwide turnover for an "enterprise," to a second level of €500,000 or 1% of annual worldwide turnover, and to a third, highest level of €1 million or 2% of annual worldwide turnover, in the most serious cases.[299] The position of the European Union Parliament in first reading in 2014, provided, in addition to the range of sanctions mentioned above, the

---

[294] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, art. 79, COM (2012) 11 final (Jan. 25, 2012).
[295] GDPR, *supra* note 1, art. 83(1).
[296] *Proposal for a Regulation*, *supra* note 294, at 2 ("[I]t is time to build a stronger and more coherent data protection framework in the EU, backed by **strong enforcement** that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.") (emphasis added).
[297] *Id*. at 5.
[298] *Id*. art. 53(4).
[299] *Id*. art. 79.

possibility of requiring "regular periodic data protection audits."[300] Furthermore, the Parliament rejected the sliding scale approach and increased the maximum level of administrative fines up to €100 million or 5% of annual worldwide turnover in the case of an enterprise.[301] This relatively radical change in fines must be seen in the context of the Edward Snowden revelations about the cooperation of U.S. Tech Giants in NSA mass surveillance programs, which were brought to the attention of the general public through the press less than one year earlier.[302] Following the trialogue negotiations among the Council, the Commission and the Parliament, the GDPR provision was modified and a two-level set of fines was adopted.

As finally provided in the GDPR, the level of administrative sanctions may vary on a case-to-case basis, depending on the circumstances, including compliance measures taken.[303] Furthermore, sanctions will differ depending on whether the controller or processor, as applicable, is an undertaking or not. An "undertaking" is a term used throughout the GDPR, but without definition.[304] It should be read to be an enterprise involved in economic activity and will often act as a legal person (or corporate entity).[305] A company (or corporation) involved in economic activity would be an undertaking. The term "enterprise" is defined as "a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity."[306]

Infringements of different categories of obligations may lead to different levels of sanctions, from up to €10 million or €20 million, in the case that the controller or processor is not an undertaking, and

---

[300] Protection of Individuals with Regard to the Processing of Personal Data, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), art. 79(2a)(b).

[301] *Id*. art. 79(2a)(c).

[302] For a discussion of the impact of the NSA revelations on the GDPR legislative process, *see* W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17 J. INTERNET L. 1, 19–21 (2014).

[303] GDPR, *supra* note 1, art. 83(2).

[304] However, the term "group of undertakings" is defined and means: "a controlling undertaking and its controlled undertakings." *Id*. art. 4(19). Obviously, this does not help us with the definition of "undertaking."

[305] In recital 14 we learn that undertakings may be established as legal persons. *Id*. recital 14. More importantly, in recital 110 we see that "group of undertakings" may be synonymous with "group of enterprises engaged in a joint economic activity." *Id*. recital 110.

[306] *Id*. art. 4(18).

up to the greater of whichever of such sums is applicable to its category and 2% or 4% of total worldwide annual turnover for preceding financial year, depending on the category, in the case of an undertaking. The two categories of provisions set out in Article 83 of the GDPR may be broken down into those the infringement of which is less serious, and those the infringement of which are more serious. The less serious include infringement of provisions centered around compliance-ensuring obligations, including specific security obligations.[307] The more serious include infringement of provisions centered around basic obligations to process data, and data subjects' rights.[308]

Perhaps what is most notable about this, in addition to the potential quantum of the fines, is that the GDPR embraces what has been described as "wealth-based punishment," which Professors Rustad and Koenig claim is a U.S. innovation,[309] not traditionally levied in the European Union.[310] Rustad and Koenig do, however, recognize the large amounts of wealth-based fines imposed by the European Commission for EU competition law violations.[311] In cases of an illegal cartel or abuse of a dominant position, fines may go up to a maximum of ten percent of total turnover of the undertaking or the association of undertakings in the preceding business year,[312] or up to two and one-half times the maximum amount under the GDPR. Through their mutual adoption of wealth-based punishment, the GDPR's tie to one area of economic law—competition law—is recognized.

The sanctioning power conferred on DPAs is part of the more general trend of European law to strengthen sanctions serving a more effective market regulation.[313] A set of common rules at European level

---

[307] *Id*. art. 83(4).
[308] *Id*. art. 83(5).
[309] *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 369, 431 (2019) (where the authors claim that the GDPR's fines are "[s]imilar to U.S. punitive damages," in that they are imposed "based upon the wrongdoer's annual turnover.") *Id*. at 431.
[310] *Id*. at 429.
[311] *Id*. at 429–31 (citing the July 2018, $5.1 billion fine against Google, the May 2009, €1.06 billion fine against Intel, and the September 2017, €2.2 billion fine against Google).
[312] Council Regulation 1/2003, art. 23(2), 2003 O.J. (L 1) 1, 17.
[313] One note focuses on "an observable intersection of data protection and competition law to create a more efficient regulatory environment with the goal of offering consumers the best protection for their personal data at the least cost for the companies storing and processing that data," which should be the goal of such trend. *See* Olivia Altmayer, *The Tipping Point –*

on sanctions is gradually being developed. The standard of "effective, dissuasive and proportionate" sanctions is present in different regulations and its understanding in the field of data protection law can therefore be inspired by its application in other areas, such as competition law or market abuse law. The power of sanctions in data protection law has been presented as a revolution, but it may also appear as the effect of a convergence between the different European regulations on sanctions.

2. The One-Stop Shop Mechanism

A "one-stop shop" (OSS) mechanism has been provided in the GDPR, whereby, when a data controller has more than one establishment in the European Union (actually the EEA), and there is cross-border processing of personal data, the DPA of the main establishment has the competence to act as "lead supervisory authority" for such cross-border processing.[314] The term "main establishment" is defined as follows:

> (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decision is to be considered to be the main establishment;
>
> (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the

Reevaluating the ASNEF-EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach, 39 NW. J. INT'L L. & BUS. 37, 40 (2018).

[314] GDPR, *supra* note 1, art. 56(1) ("Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.").

> extent that the processor is subject to specific obligations under this Regulation[.][315]

The term "place of its central administration" is not defined in the GDPR but may be seen as the place out of which the company is actually run, where the main decisions are made, usually corresponding to the operational headquarters.[316] Yet, cases may exist "where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity" where there could be more than one lead DPA.[317]

In this context, "cross-border processing" means either "processing of personal data which takes place in the context of the activities of the establishment in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State"[318] or "processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."[319] In other words, there is an element of internationality either through the places where processing takes place in the context of a controller's or processor's establishments' activities, or where there is a single establishment but their processing affects data subjects in different EU Member States. Additionally, the DPA, who has the lead role, may change if there is the relocation of a company's main establishment to another EEA Member State, and if there is an ongoing procedure involving that company. This would "deprive the first authority of its original competence at the moment such a change becomes effective, but not to retrospectively deprive the operations

---

[315] *Id*. art. 4(16).

[316] *See* Luca Tosoni, *Article 4(16). Main establishment*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 225, 230 (Christopher Kuner et al. eds., 2020).

[317] Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 rev.01, adopted on Dec. 13, 2016, as last revised and adopted on Apr. 5, 2017 [hereinafter WP 244] (this would be the case, "where a multinational company decides to have separate decision making centres, in different countries, for different processing activities."). These Guidelines were endorsed by the EDPB when it came into existence and replaced the Article 29 Data Protection Working Party on May 25, 2018. European Data Protection Board, Endorsement 1/2018, at 2 (May 25, 2018).

[318] GDPR, *supra* note 1, art. 4(23)(a).

[319] *Id*. art. 4(23)(b).

already carried out by the initial authority of a legal basis."[320] Thus, the DPA of the new Member State where the main establishment is located would become the lead DPA.

However, despite this competence of the lead DPA, each DPA may handle complaints brought to it or possible GDPR violations if related only to the establishment in its Member State or where it substantially only affects data subjects there,[321] after having informed the lead supervisory authority,[322] where the lead supervisory authority does not decide to handle the case, subject to procedures of mutual assistance and joint operations between the DPAs.[323] Where the lead supervisory authority decides to handle the case, the procedure for cooperation between itself and the other "supervisory authorities concerned" shall apply.[324] In any case, the lead DPA is "the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor,"[325] although it has been suggested that this does not mean that the lead DPA must be their sole contact point.[326] Furthermore, there is a consistency mechanism set up under the GDPR,[327] in which the EDPB takes a key

---

[320] European Data Protection Board, Opinion 8/2019, at 8 (July 9, 2019) (On the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment).

[321] GDPR, *supra* note 1, art. 56(2) ("By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.").

[322] *Id.* art. 56(3).

[323] *Id.* art. 56(5).

[324] *Id.* art. 56(4) (the cooperation procedure is set out in Article 60 of the GDPR). "Supervisory authority concerned" is defined as "a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority." *Id.* art. 4(22).

[325] *Id.* art. 56(6).

[326] HIELKE HIJMANS, *Article Commentary*, *Art. 56 Competence of the Lead Supervisory Authority*, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 913, 924 (Christopher Kuner et al. eds., 2020) ("This does not mean that the lead DPA must always operate as the sole contact point of the local DPA. In view of the strong position of the local DPA on substance, as described, it would be illogical to preclude the local DPA from interacting with the controller or processor.").

[327] GDPR, *supra* note 1, art. 63.

role through, for example, issuing opinions[328] or adopting binding decisions to resolve disputes.[329]

As a result of this OSS mechanism, the sanctioning power of the supervisory authorities is exercised on a national (or Member State) level, through Member State DPAs,[330] whether they be lead supervisory authorities or supervisory authorities concerned, albeit with a coherency mechanism headed up by the EDPB. This may be seen to go against the trend for enforcement more generally in the European Union, which is a move of enforcement powers from the Member States to the European Union.[331] This trend is illustrated, for example, by changes in the supervisory competence of large financial institutions. In the past, credit institutions in the Member States were regulated by national supervisory authorities, irrespective of their size. Today, the main European banking groups are mainly placed under the supervision of the European Central Bank, which has, *inter alia*, the power to impose administrative sanctions (up to 10 % of the total annual turnover).[332] It may be argued that the fact that administrative sanctions under the GDPR are handled at the Member State level, through national DPAs, especially when the position of Ireland is considered, is the root of difficulties for the enforcement of the GDPR, as discussed in Section 3 below.

3. Comparison with Sanctions Prior to the Application of the GDPR

Immediately prior to the application of the GDPR, maximum fines under Member State national law implementing the EU DP Directive did not generally exceed hundreds of thousands of euros. For example, in Germany the maximum was €300,000; in the United Kingdom, it was £500,000 or roughly €580,000; in Sweden, one million crowns or roughly €105,000; in Ireland €100,000; in Italy,

---

[328] *Id.* art. 64.
[329] *Id.* art. 65.
[330] *See* Commission Decision of June 27, 2017, *supra* note 51 (Provides a definition of "supervisory authority." This study uses the abbreviation DPA for "supervisory authority" as well).
[331] *See* Scholten et al., *supra* note 66, at 6 ("[. . .] a clear trend has emerged where enforcement powers that were once in the hands of the MS have been transferred to the EU").
[332] Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, art. 18 (2013).

€300,000; in the Netherlands, €820,000 or 10% of turnover; in Romania €22,000 or 2% of turnover; and in France €3,000,000.[333]

After the application of the GDPR, on March 14, 2019, the Dutch DPA—*Autoriteit Persoonsgegevens*—published a fining structure for GDPR violations and those of the Netherland's implementing act for the GDPR, introducing four fine categories with fine ranges extending from €0-€200,000 to €450,000-€1 million and default fine rates ranging from €100,000 to €725,000.[334] Although these rates differ from the GDPR rates (and indeed are much lower than those in the GDPR[335]), the Dutch DPA may vary its fines from the default rates based on mitigating or aggravating factors and may still fine up to the maximum fine rates set out in the GDPR.[336] This highlights the principle that fines must at the same time dissuade, be effective and not be disproportionate, so that the circumstances of each case must be evaluated before establishing the fine, but it also may be sending a clear message that "fines are coming!"[337] If the EDPB were to decide to publication guidelines for the calculation of GDPR fines, however, the Dutch DPA might withdraw its guidelines.[338]

While the first six months to one year following the first date of application of the GDPR seemed to be a relative "cease-fire," this changed with a first multimillion euro fine by the French DPA against

---

[333] *See* BART CUSTERS ET AL., EU PERSONAL DATA PROTECTION IN POLICY AND PRACTICE 228 (2019). Note that, in France's case, maximum fines had been €150,000 for first offenses until adoption of the GDPR, but during the period between the GDPR's adoption and its application this was changed by the *Loi pour une République numérique* (Digital Republic Act) of October 7, 2016, which increased maximum fines to €3,000,000, thus anticipating higher fines under the GDPR. *See* CNIL, *Ce que change la loi pour une République numérique pour la protection des données personnelles* [What the Digital Republic Act Changes for the Protection of Personal Data] (Nov. 17, 2016), https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles.

[334] Steenbruggen et al., *Dutch Regulator Publishes Guidelines for the Calculation of Administrative Fines Under the GDPR*, BIRD & BIRD (Apr. 2019), https://www.twobirds.com/en/news/articles/2019/netherlands/dutch-regulators-publishes-guidelines-for-the-calculation-of-administrative-fines-under-the-gdpr.20.

[335] *Id.*

[336] *Id.*

[337] *Id.* (the authors suggest that if the EDPB decides to publish guidelines for the calculation of GDPR fines, the Dutch DPA might withdraw its guidelines).

[338] *Id.*

Google in January 2019.[339] While only amounting to 0.05 % of revenue for Google's parent, Alphabet, for the year 2017,[340] such fine for violations of the obligations of transparency and information, and for lack of a legal basis for ads personalization data processing is, as of October 31, 2020, the largest fine issued under the GDPR. However, more spectacularly, in July 2019, the United Kingdom's DPA—the ICO—announced intentions to fine British Airways £183.39 million[341] and Marriott International more than £99 million,[342] both in connection with data breaches. However, the British Airways fine was eventually lowered to £20 million,[343] and the Marriott International figure was finally reduced to £18.4 million.[344] As of October 31, 2020, fourteen fines of over €1 million have been assessed by an EU or EEA DPA since the GDPR has applied: (i) Google LLC (France), €50,000,000; (ii) Hennes & Mauritz Online Shop A.B. & Co. KG (Germany), €35,258,708; (iii) TIM (Italy), €27,800,000; (iv) British Airways (United Kindgom), €22,046,000; (v) Marriot International, €20,450,000; (vi) Austrian Post (Austria), €18,000,000; (vii) Wind Tre S.p.A. (Italy), €16,700,000; (viii) Deutsche Wohnen SE (Germany),

---

[339] *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (the fine amounted to €50 million and was appealed, unsuccessfully, by Google).

[340] The CNIL converted the 2017 revenue of Alphabet—$109.7 billion—into the figure of roughly €96 billion. *See* Commission Nationale de l'Informatique et des Libertés, *Délibération n°SAN-2019-001 du 21 janvier 2019*, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1 (Fr.). Dividing the amount of the fine by this revenue figure yields roughly 0.05%. Note that the sanction was upheld on appeal by the Council of State (CE 19 June 2019, req. n° 430810), https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/430810.

[341] *Intention to Fine British Airways £183.39m Under GDPR for Data Breach,* ICO (July 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

[342] *Intention to Fine Marriott International, Inc More than £99 Million Under GDPR for Data Breach*, ICO (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

[343] *British Airways*, ICO (Oct. 16, 2020), https://ico.org.uk/action-weve-taken/enforcement/british-airways/.

[344] *Marriott International Inc*, ICO (Oct. 30, 2020), https://ico.org.uk/action-weve-taken/enforcement/marriott-international-inc/.

€14,500,000; (ix) 1&1 Telecom GmbH (Germany), €9,550,000; (x) Eni Gas e Luce (Italy), €8,500,000; (xi) €3,000,000; (xii) Google LLC (Sweden), €7,000,000; (xiii) National Revenue Agency (Bulgaria), €2,600,000; and (xiv) Allgemeine Ortskrankenkasse (Germany), €1,240,000.[345] Other than the CNIL Google fine and the Data Protection Authority of Sweden Google fine, the only four other fines of a U.S. Tech Giant are a Data Protection Authority of Hamburg fine assessed on Facebook Germany GmbH in the amount of €51,000,[346] far below the maximum fine that could have been assessed,[347] a more recent Belgian DPA (Autorité de protection des données (APD)) fine imposed on Google Belgium SA, in the amount of €600,000;[348] and a Hungarian DPA fine of Google Ireland Ltd. in the amount of €58.[349] Thus, while a few multimillion euro fines have been assessed, there has not been a fine of a U.S. Tech Giant in the hundreds of millions of euros, much less in the billions. However, the larger fines do benefit from the increased maximum levels allowed by the GDPR, as do even the intermediate fines. This analysis is important, although not enough, as indicated by the Committee on Civil Liberties, Justice and Home Affairs (known as the LIBE Committee) of the European Parliament, which called for the following:

---

[345] *See* GDPR Enforcement Tracker, CMS, https://enforcementtracker.com (last visited on July 8, 2020) (this listing of GDPR fines is compiled by global law firm CMS, through its German member CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB).

[346] *Id.*

[347] *See* Facebook Germany GmbH, DUN & BRADSTREET (last visited on July 13, 2020), https://www.dnb.com/business-directory/company-profiles.facebook_germany_gmbh.84c0ca792f206051f23fa9d29059a699.html (In 2017, Facebook Germany GmbH revenue was $42.05 million). Based only on the revenue of the German subsidiary, the maximum fine for a first offense by a company would be either $10 million or $20 million, depending on the category of the violation. If assessed on Google segment revenue of Alphabet Inc., the figure increases dramatically, as the 2019 revenue was $160.74 billion. *Annual revenue of Google from 2002 to 2019*, STATISTA (last visited on Oct. 21, 2020), https://www.statista.com/statistics/266206/googles-annual-global-revenue/.

[348] Autorité de protection des données, 600,000 euros d'amende: l'APD sanctionne Google Belgium pour non-respect du droit à l'oubli [600,000 Euros Fine: APD Sanctions Google Belgium for Non-Compliance with the Right to be Forgotten] (July 14, 2020), https://www.autoriteprotectiondonnees.be/news/600000-euros-d-amende-l-apd-sanctionne-google-belgium-pour-non-respect-du-droit-a-l-oubli.

[349] *See id.*

> Regarding the level of enforcement and specifically the sanctions foreseen under the GDPR, an evaluation of the appropriateness and the effectiveness of the fines issued in relation to the violations of the GDPR should be conducted. For this purpose, the sanctions issued for infringements of the GDPR should be broken down by category, by industry and by size of business. Any calculation mechanism used by DPAs would show the enforcement practice and could allow to give an indication of the proportion of sanctions/fines issued in relation to reported breaches. Furthermore, since several DPAs have started imposing fines on data controllers, it would be relevant to assess the impact of fines issued in relation to the violations of the GDPR and whether the fines have led to subsequent compliance.[350]

Nonetheless, the DPA of one very important jurisdiction, Ireland, where many U.S. Tech Giants have their EU headquarters, in July 2019, was reported to have eleven investigations underway for Facebook violations of the GDPR, with at least two rulings likely in the then-coming months.[351] The Irish Commissioner for Data Protection—Helen Dixon—underscored both the Irish DPA's role in public enforcement of the GDPR and in providing guidance to companies so that they may comply with the law. Speaking about the second year of the GDPR's application, the Irish DPA stated that the conclusion of ongoing investigations will "showcase how the corrective and fining powers afforded to data protection authorities can be utilized."[352] Of the nineteen ongoing "statutory inquiries" in Ireland, most concern the U.S. Tech Giants and their subsidiaries: Facebook counts for a total of eleven (eight for the parent, two for WhatsApp,

---

[350] Annex to the Letter of the LIBE Committee of the European Parliament of 21 February 2020 to Commissioner Reynders, Ref: IPOL-COM-LIBE D (2020)6525 at 4, https://www.politico.eu/wp-content/uploads/2020/03/SKM_C45820030616021.pdf.

[351] *See* Adam Satariano, *Facebook Dodged a Bullet from the F.T.C. It Faces Many More.*, N.Y. TIMES (July 13, 2019), https://nyti.ms/30xFwm0 (the Irish DPA is also reported to have been investigating Google). Note that, as of June 30, 2020, those two rulings had not yet been issued.

[352] Press Release, Data Protection Commission, Data Protection Commission Reflects on the First Year of the GDPR (May 24, 2019), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-reflects-first-year-gdpr.

and one for Instagram); Apple for two; Google for one; and Microsoft subsidiary LinkedIn for one. Of the remaining cases, Twitter accounts for three and Quantcast for one.[353]

The Irish DPA itself reported that it had received 6,624 complaints in the GDPR's first year,[354] and that it would conclude investigations within the GDPR's second year, including those involving certain internet platforms.[355] In addition to Google, Apple and Twitter were named.[356] However, as of June 30, 2020, the Irish DPA had assessed only two fines, each on Tusla Child and Family Agency, in the amounts of €75,000 and €40,000, respectively, and both assessed in the second quarter of 2020.[357] As of that date, no data protection fine under the GDPR had been imposed by Ireland on a U.S. Tech Giant.

D. EU Institutional Reactions to GDPR Enforcement and GDPR Cooperation and Consistency Mechanisms

The European Commission described the "lack of blockbuster fines" during the GDPR's first year as nothing to be concerned about.[358] It qualified national data protection authorities' actions as a "balanced approach to enforcement powers," adding that "[t]hey have focused on dialogue rather than sanctions, in particular for the smallest operators which do not process personal data as a core activity."[359] The Commission indicated that some of the delay in action was due to

---

[353] *See* Simon Carswell, *GDPR One Year On: No Fines But Considerable Amounts of Dread*, IRISH TIMES (May 25, 2019), https://www.irishtimes.com/business/technology/gdpr-one-year-on-no-fines-but-considerable-amounts-of-dread-1.3903169.

[354] *See id*. As a point of comparison, the French regulator (CNIL) indicated in its activity report for 2019 that it had received 14,000 complaints during the year, an increase of more than 27% compared with the previous year, of which 20% were cross-border complaints. *See Rapport d'activité 2019*, CNIL, (June 2020) https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf.

[355] *See* Press Release, Data Protection Commission, *supra* note 352.

[356] *See* Carswell, *supra* note 353.

[357] *See* GDPR Enforcement Tracker, *supra* note 345.

[358] *See* Mehreen Khan, *Brussels Defends Lack of Blockbuster Fines for Big Tech Groups*, FIN. TIMES (July 23, 2019), https://www.ft.com/content/3629b0fc-ad73-11e9-8030-530adfa879c2. This view has been echoed more recently: *see* Catherine Stupp, *EU Privacy Regulators Found to Lack Staff, Funds to Enforce GDPR*, WSJ PRO CYBERSECURITY (June 29, 2020, 5:30 AM ET), https://www.wsj.com/articles/eu-privacy-regulators-found-to-lack-staff-funds-to-enforce-gdpr-11593423000.

[359] *See Data Protection Rules as a Trust-Enabler*, *supra* note 284, at 4.

DPAs wanting to ensure that they have cases that respect procedure, and it also focused on the change in culture and behavior of relevant actors as a sign of success.[360] Furthermore, concern was expressed about whether the DPAs have the necessary resources to bring the big cases.[361] The preference given to educational action during the implementation phase of the new regulation with dissuasive sanctions is quite typical of a regulatory approach to sanctions.[362] Nevertheless, certain hypotheses (lack of resources, reluctance to initiate proceedings, etc.) put forward by the Commission suggest that the practice of national regulators' supervisory and sanctioning powers does not allow sanctions to play their full role.[363]

The GDPR itself calls for a report by the Commission on an evaluation and review of that regulation, particularly covering cross-border personal data transfers and cooperation and consistency mechanisms involving the DPAs and the EDPB by May 25, 2020, and every four years thereafter.[364] On January 21, 2020, the Council adopted[365] its position and findings on the application of the General Data Protection Regulation (Council Position),[366] meant to contribute to the Commission's 2020 review. In the Council considered that cooperation be strengthened between Member State Supervisory Authorities, "as it is particularly relevant for the supervision of cross-border processing involving risks or for the processing concerning many Member States, for instance as regards so-called big tech companies."[367] However, the Council found that it was too early to assess the functioning of GDPR's cooperation and consistency mechanisms.[368]

The EDPB also contributed to the discussion around the Commission's GDPR evaluation and review in a document adopted on

---

[360] *Id.* at 5.
[361] *See* Khan, *supra* note 358.
[362] *See* Arnaud Lecourt, *RGPD*: *nouvelles contraintes, nouvelles stratégies pour les entreprises*, 2019 DALLOZ IP/IT 205 (Apr. 9, 2019) (commenting on the pedagogical role of the CNIL from the start).
[363] *See* Nemitz, *supra* note 58, at 2.
[364] GDPR, *supra* note 1, art. 97(1)–(2).
[365] Council of the European Union Brussels Press release 5332/20, Outcome of the Council Meeting, 3743rd Council Meeting, Economic and Financial Affairs (Jan. 21, 2020).
[366] Council of the European Union Brussels 'A' Item Note, Council Position and Findings on the Application of the General Data Protection Regulation (GDPR), 14994/2/19 REV 2 (Jan. 15, 2020).
[367] *Id.* at 5.
[368] *Id.* at 10.

February 18, 2020.[369] It noted that the divergence of national procedures and practices negatively impacted the cooperation and consistency mechanisms, and that Supervisory Authority resources were insufficient.[370] Furthermore, consistent interpretation of GDPR terms is needed, among other concerns.[371] However, it is clear that the cooperation and consistency mechanisms are still in a breaking-in period and, for example, the joint operation procedure under Article 62 of the GDPR has not yet been triggered by the Supervisory Authorities,[372] and the dispute resolution procedure set forth in Article 65 of the GDPR has not led to the adoption of a binding decision as, "so far the involved SAs have been able to reach consensus on cross-border cases in the cooperation mechanism."[373]

During the period from May 25, 2018 to December 31, 2019, 1346 procedures were initiated to identify the Lead Supervisory Authority (and also the Concerned Supervisory Authorities) for the OSS, and cases with a cross-border element were registered in the central Internal Market Information (IMI) Case register database.[374] During the same period, 807 cases were registered in the IMI database, for which the following countries were the six countries serving as Lead Supervisory Authority for the largest amount of cases: Ireland (127 cases), Germany (92 cases), Luxembourg (87 cases), France (64 cases), the United Kingdom (56 cases), and the Netherlands (45 cases).[375] As noted by the Commission, the "ranking reflects notably the specific situation of Ireland and Luxembourg, who host several big multinational tech companies,"[376] notably those this study refers to as the U.S. Big Tech Companies.

A further contribution to the Commission's evaluation was made by an expert group that it set up, including business associations, civil society associations, and individual professional or academic

---

[369] EDPB, *supra* note 250.
[370] *Id.* at 3.
[371] *Id.* at 12.
[372] *Id.* at 14.
[373] *Id.* at 17.
[374] *Id.* at 7.
[375] EDPB, *supra* note 250, at 8.
[376] European Commission, Commission Staff Working Document Accompanying the Document Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizens' Empowerment Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years Digital Transition – Two Years of Application of the General Data Protection Regulation, at 7, SWD(2020) 115 final (June 24, 2020).

members (Multistakeholder Expert Group).[377] In its report, the Multistakeholder Expert Group highlighted the need to prevent fragmentation in application of the GDPR rules,[378] and its civil society members called for "stronger and more coordinated enforcement of the data protection rules by DPAs."[379] Several comments were made about enforcement actions: although not consistent in all sectors, an increase in complaints to DPAs was noted; however there was no significant increase in court actions caused by the GDPR.[380]

Several uses of representative actions under Article 80 of the GDPR were remarked in the report, where civil society and consumer organizations acted, generally under a mandate from individuals: (i) NOYB and LQDN complaints filed on the first day of application of the GDPR with several DPAs against U.S. Tech Giants Google, Amazon, Facebook, Apple and Microsoft;[381] (ii) a coordinated action by consumer organizations against Google launched in November

---

[377] Contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation (GDPR), Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, Report, at 3–4 (June 17, 2020), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=41708, [hereinafter Expert Group Report].

[378] *Id.* at 5.

[379] *Id.*

[380] *Id.* at 13 ("Several members reported complaints related to transparency obligations, consent, request for identification by the controller before responding to a data subject's request, and the exercise of data subjects' rights in particular the right of access… Most business members indicate that there was either no court action or no significant increase in the number of court actions against their members' organisations caused by the GDPR").

[381] *Id*. at 14 (these complaints were centered on the issue of consent). A couple of these complaints resulted in the CNIL's largest administrative fine so far, in the Google LLC case discussed in Part III.A.2.b. One law firm commented that, "This indicates that if a well-known not-for-profit organization lodges a basic but sufficiently argued claim, it might be sufficient for a data protection authority to launch an investigation. Also, the success of the collective complaint of this case may encourage data subjects to utilize a collective complaint and/or redress mechanism provided for under Article 80 GDPR." Romain Perray, *Euro Fifty Million GDPR Fine on Google by French Data Protection Authority*, LEXOLOGY (July 9, 2019), https://www.lexology.com/library/detail.aspx?g=67739262-9e11-4664-ac72-1576414b9e48 (the author also mentioned that the case was carried out entirely online, without on-site inspect, leading him to conclude that, "A data protection authority may now easily investigate digital businesses even if their offices are located outside its geographical jurisdiction," increasing risk of investigations for global digital business).

2018, involved the filing of complaints regarding the processing of location data with the DPAs of Norway, Sweden, the Netherlands, Slovenia, Greece, the Czech Republic and Poland;[382] (iii) Privacy International filed complaints in November 2018, as a civil society organization, without mandates of individuals, against seven data brokers and credit reference agencies for profiling without a legal basis, and for failure to comply with certain data protection principles, with DPAs in France, Ireland and the United Kingdom;[383] (iv) Open Rights Group, Panoptykon Foundation and their partners in December 2018, and January 2019, filed complaints regarding online behavioral advertising processing;[384] and (v) Norwegian consumer association Forbrukerrådet filed complaints in January 2020, in Norway regarding ad-tech processing.[385] Nonetheless, "many Member States have not made use of Article 80(2) of the GDPR, which would allow NGOs to bring forward collective complaints without having to be directly mandated by individuals,"[386] however, civil society and consumer organizations are contemplating bringing actions before courts in order to obtain compensation for data subjects.[387] Finally, response by DPAs to actions brought so far has been slow, with decisions on important cross-border cases not yet rendered.[388]

In its June 2020 communication, the Commission committed to pursuing exchanges with EU Member States regarding national DPA resources, called on the EDPB to increase cooperation among DPAs, including through joint investigations,[389] supported reflection within the EDPB on improving cooperation among the DPAs on cross-border cases, and stated that "Member States shall allocate resources to data protection authorities that are sufficient for them to perform their tasks."[390]

---

[382] Expert Group Report, *supra* note 377, at 14 (this was reported by BEUC).
[383] *Id.*
[384] *Id.* (this was reported by Access Now).
[385] *Id.*
[386] *Id.* at 15.
[387] *Id.*
[388] Expert Group Report, *supra* note 377, at 15–16.
[389] *Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years Digital Transition – Two Years of Application of the General Data Protection Regulation*, at 15, COM(2020) 264 final (June 24, 2020), https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf.
[390] *Id.* at 16.

E. Conclusion on GDPR Sanctions

In this study's Introduction, the question was asked, *does the reality of supervisory authority action support the theoretical goals for GDPR sanctions?* In Part I this study discussed the goals of sanctions to include the main objective of acting as a deterrent, providing an incentive for companies to comply with the regulations. However, other functions for sanctions exist: the incapacitation effect; the budgetary effect; the normative and symbolic effect; the consolidation of the market by weakening an artificially dominant actor effect, and so on. However, this study has shown that the deterrence effect is perhaps the most important sub-goal of sanctions in the context of GDPR sanctions, with the symbolic function also playing an important role.

From today's viewpoint, given the failure of Ireland and Luxembourg to issue substantial fines on the U.S. Tech Giants, and given the relatively moderate level of fines indicated in Section C.3., the answer has to be that the reality of GDPR sanctions has not yet supported the theoretical goals of GDPR sanctions—especially the deterrence and symbolic sub-goals—which to a fairly large extent require effective and substantial sanctions. Furthermore, although the combination of action on the competition, data protection and consumer protection fronts has provided the strongest challenge to U.S. Tech Giants so far, doubts have been expressed about the ability of "mere fines" to help bring them into rein.[391] However, the enforcement toolbox has expanded considerably, and collective action provides possibilities for individuals to more easily bring complaints. In this context, this study now investigates strategic aspects and risks.

III. STRATEGIC ASPECTS AND RISKS: LACK OF UNDERSTANDING OF THE GDPR, NON-COMPLIANCE AND NON-ENFORCEMENT

As part of its investigation of the impact of sanctions, this study will analyze strategic aspects and risks, first from the standpoint of companies,[392] which may react in an incorrect way, either through a lack of understanding of the GDPR, or through a conscious decision to

---

[391] *See* Julia Powles, *The EU is Right to Take on Facebook, But Mere Fines Don't Protect Us from Tech Giants*, Guardian (May 27, 2017), https://www.theguardian.com/commentisfree/2017/may/20/eu-right-to-take-on-facebook-fines-dont-protect-us-from-tech-giants (stating, in this opinion piece, that "[i]If we are really to change the dynamics of the modern data economy, it is going to take more than just targeted arrows and small-fry fines. The true response to Facebook is to see it as a company that ruthlessly monetizes every aspect of our everyday lives.").

[392] Lecourt, *supra* note 362.

try to game the system or to fail to comply (Section A), before looking at the risks of non-enforcement by DPAs and the effect this may have on companies (Section B).

A. Risks Involved with Lack of Understanding of the GDPR and Non-Compliance

Firms faced with decisions regarding the processing of personal data might, for lack of understanding of the provisions of the GDPR, prove too zealous or even fail to comply with the legislation. Furthermore, companies may be tempted, given the GDPR enforcement record of the European DPAs to data, to assume greater risks with respect to non-compliance, or to try to arbitrage based on the position of the various DPAs to date. However, this study argues that such reactions would be poor corporate strategy. In order to analyze these risks and strategic aspects, focusing on the action of companies, this study engages the legal strategy and compliance literature. This Part begins with a short discussion of legal strategy and competitive advantage (Section 1), then analyzes certain aspects of understanding the GDPR (Section 2), prior to discussing compliance, non-compliance, and sanctions (Section 3).

1. Legal Strategy and Competitive Advantage

Strategy theory informs us that, at least in emerging industries outside of "a traditionally regulated sphere" regulation may be imposed abruptly, slowing the industry's progress.[393] The U.S. Tech Giants, based in a culture where entrepreneurs live by the mantra, "Move fast and break things," attributed to Facebook's Mark Zuckerberg,[394] have developed in a legal culture where there has been meager protection of data privacy.[395] Arguably, this has given them a competitive advantage over companies from jurisdictions such as the European Union, where certain actions are prohibited or restrained by data protection law. In the legal strategy literature, while the baseline discussion relates to what behavior is illegal, mere compliance is considered a limiting position, compared to the use of law proactively, to create and capture

---

[393] MICHAEL E. PORTER, COMPETITIVE STRATEGY: TECHNIQUES FOR ANALYZING INDUSTRIES AND COMPETITORS, 224 (1st ed. 1980).

[394] Hemant Taneja, *The Era of "Move Fast and Break Things" Is Over*, HARV. BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over.

[395] *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 642 (2014). *See also* W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 491–92 (2020).

value and obtain competitive advantage.[396] Seidel and Haapio discuss the diminishment of legal comparative advantage as a result of convergence of substantive and procedural law globally.[397] While Seidel and Haapio cite several fields of law for which this is the case (contract, product liability, environmental law, securities regulation, and sexual harassment),[398] data protection or data privacy law does not figure on their list. Data privacy law has not been harmonized internationally, especially not between the United States and the European Union.[399] However, one of the arguably subsidiary aims of the GDPR[400] has been to eliminate what has been seen as an element of competitive advantage of U.S. Tech Giants by levelling the playing field between European companies and non-European ones such as the U.S. Tech Giants[401] in the area of data privacy. The GDPR, with its extraterritorial effect, may be considered the abrupt imposition of regulation on the U.S. Tech Giants (unless they scrupulously renounce

---

[396] *See* Constance E. Bagley, *What's Law Got to Do with It?: Integrating Law and Strategy*, 47 AM. BUS. L.J. 587, 587–88 (2010).

[397] George J. Siedel & Helena Haapio, *Using Proactive Law for Competitive Advantage*, 47 AM. BUS. L.J. 641, 645 (2010).

[398] *Id*. at 645–46.

[399] *See* W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 408–12 (2019).

[400] The GDPR's stated objectives are twofold:

> 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
>
> 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

GDPR, *supra* note 1, art. 1(2)–(3).

[401] *See, e.g., Questions and Answers – General Data Protection Regulation*, EUR. COMM'N (Jan. 24, 2018), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 ("The same rules for all companies – regardless of where they are established: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business in our Single Market. With the reform, companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market. This creates a level playing field.") (emphasis omitted). *See also* Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies*, 11 HASTINGS SCI. & TECH. L.J. 101, 124 (2020) ("In Europe, the aspect of the new approach that received the most praise was the equality of competition between companies in and outside of the European Union.") (citation omitted).

the European market that is not realistic) of which the strategy theory spoke.

2. Understanding the GDPR: Management Understanding of the Law

Seidel has set out an action plan for achieving competitive advantage, called the "Manager's Legal Plan," the first of four steps of which is "management understanding of the law."[402] A manager must have an understanding of the law in order to implement further steps in order to obtain competitive advantage.[403] This is important with respect to an American company faced with GDPR compliance because of major differences between the EU and U.S. law,[404] including even differences in terminology and concepts.[405] This Section illustrates the importance of management understanding the law through two cases: first, this study discusses the understanding of the law and risks of over-compliance (Section a), before discussing management understanding of the OSS mechanism (and the concept of "main establishment") and efforts to forum shop (Section b).

a. Over-Compliance

Bagley informs us that lawyers may be incentivized to "overstate legal risk," and be overly conservative, such as when faced

---

[402] *See* Siedel & Haapio, *supra* note 397, at 651–52 (discussing Siedel's Manager's Legal Plan); *see* Siedel, *Using the Law for Competitive Advantage*, 20–25 (2002).

[403] *See* Siedel & Haapio, *supra* note 397, at 651.

[404] *See, e.g.,* Voss, *supra* note 399, at 417–27 (discussing the lack of harmonization between EU and U.S. "data privacy" law).

[405] *See generally* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014) (examples regarding the differences between the concepts and terms of "personal data" in the European Union, and "personal information" or "personally-identifiable information (PII)" in the United States); *see also* Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud?: A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 422–32 (2013) (regarding the differences in the concept of "sensitive data" or "sensitive information" between the European Union—which actually refers to "special categories of data"—and the United States); *see also* Voss & Houser, *supra* note 22, at 310, 321 (on a U.S. view of sensitive data and on sensitive data in the European Union); and *see* Voss, *supra* note 399, at 408–09 (on the difference in terminology among the terms "privacy," "data privacy," and "data protection.").

with "high ambiguity,"[406] which may be the case in the early years of the GDPR's application. Top management familiarity with the GDPR and DPA guidance may help them be what Bagley describes as "legally astute,"[407] allowing them to treat the GDPR as a business issue with a business solution. Bird and Park discuss using corporate compliance to obtain competitive advantage, acknowledging that different firms have different profiles where compliance is concerned, and arguing that firms may tend to over-comply with regulation out of a "disproportionate fear of sanction."[408] This may be the case with data protection breach reporting under the GDPR, which does not require a notification to the DPA if the "data breach is unlikely to result in a risk to the rights and freedoms of natural persons,"[409] for example, where data have been properly encrypted so that unauthorized parties are unable to read them.[410] As stated by the ICO's Deputy Commissioner (Operations) in 2018,

> Some controllers are "over-reporting": reporting a breach just to be transparent, because they want to manage their perceived risk or because they think that everything needs to be reported. We understand this will be an issue in the early months of a new system but we will be working with

---

[406] Constance E. Bagley, *Winning Legally: The Value of Legal Astuteness*, 33 ACAD. MGMT. REV. 378, 382 (2008).
[407] *Id*.
[408] Robert C. Bird & Stephen Kim Park, *Turning Corporate Compliance Into Competitive Advantage*, 19 U. PA. J. BUS. L. 285, 310 (2017) (citation omitted).
[409] GDPR, *supra* note 1, art. 33(1).
[410] Cédric Burton, *Article 33. Notification of a Personal Data Personal Data Breach to the Supervisory Authority*, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 640, 647 (Christopher Kuner et al., 2020) ("The WP29 has also given examples of situations where the rights and freedoms of natural persons are not at issue, such as where the personal data are already publicly available and their disclosure does not present a likely risk to the individuals concerned, and when data have been properly encrypted so that they have been made unintelligible to unauthorised parties and a copy or a backup exists") (citing Article 29 Data Protection. Working Party, Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250rev.01, as last revised and adopted on Feb. 6, 2018, at 18–19), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Those Guidelines were endorsed by the GDPR. *See Personal Data Breach Notifications*, EUROPEAN DATA PROTECTION BOARD (May 25, 2018), https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_en (GDPR endorsing those guidelines).

> organisations to try and discourage this in future once we are all more familiar with the new threshold.[411]

A greater understanding of the GDPR's data breach notification requirements could help alleviate this issue, for example, and the ICO has published self-assessment tools to help achieve this.[412] DPA guidance is an effective source of material that may help management to better understand compliance issues. With regard to the expressive function of sanctions, we have noted that some DPAs may be tempted to impose sanctions more particularly against emblematic companies such as U.S. tech giants. Then the problem of over-compliance should be considered by companies in relation to their risk of being subject to exemplary sanctions because of their notoriety. Larger companies may need to be more cautious than smaller or less well-known companies. It can be hypothesized that the risk of sanction related to the expressive function of sanctions is not completely independent of the way public opinion views a company. Although DPAs are supposed to be "independent" according to the GDPR,[413] this independence is understood more as an independence from governments and market players than from citizens in general, since the objective of the GDPR is to protect them in particular.[414] From this point of view, there could be an influence of public opinion and a propensity of DPAs to consider exemplary sanctions against a company. In other words, the occurrence of a scandal or circumstances affecting trust in the company (such as a major case of lack of data security, illegitimate exploitation of data for political purposes for example) could lead some DPAs to impose heavy sanctions on liable companies.

b. The OSS Mechanism and "Forum Shopping"

Another area where management could be well served by a full understanding of data protection law is with respect to the OSS mechanism. While the GDPR, through its extraterritorial scope, was intended to avoid forum shopping in the sense that had the legislation's

---

[411] ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference, INFORMATION COMMISSIONER'S OFFICE (Sept. 12, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/.

[412] *Self-Assessment for Data Breaches*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ (last visited on July 18, 2020).

[413] GDPR, *supra* note 1, art. 52.

[414] *Id*. art. 51(1).

jurisdiction been based solely in the place of the registered office of a data controller, a company might have been able to avoid the application of EU law (and thus avoid requirements for compliance) by setting up its registered office outside of the European Union,[415] it may still seem to provide a basis for forum shopping through the OSS mechanism.[416] This relates to the concept that, based on enforcement records of the GDPR to-date by the various EU Member States, U.S. and other non-EU companies may engage in legal arbitrage, choosing their forum for potential discussions of administrative sanctions using the OSS mechanism. This is arguably what the U.S. Tech Giants have already done through their choices for a jurisdiction in which to locate their EU headquarters,[417] maybe because of the perception that Ireland, given its size and the resources its DPA has available for enforcement,[418] might be a jurisdiction unlikely to be zealous in

---

[415] *See* Klar, *supra* note 401, at 124 (commenting that a "marketplace rule" for jurisdiction was chosen over this "origin rule approach").

[416] *See supra* Part II.C.2 (OSS Mechanism, noting that the term "forum shopping" may not be the perfect word choice to reflect these "forum choices"); *see also* Pamela K. Bookman, *The Unsung Virtues of Global Forum Shopping*, 92 NOTRE DAME L. REV. 579, 582 (2017) (Bookman comments that "the practice of global forum shopping is deplored but poorly defined," with critics using it as a derogatory term to refer to forum choices, instead. This study has retained the controversial term, not only because it is used in this context in the literature, but also because the forum choice determines (in many cases) the choice of lead DPA.).

[417] *See* Vinocur, *supra* note 217 (The "two nations most directly responsible for policing the tech sector" as a result of having the main tech companies having their EU headquarters there are Ireland and Luxembourg, with Ireland overseeing Google, Facebook, Microsoft and Twitter.); *see also* Adam Satariano, *New Privacy Rules Could Make This Woman One of Tech's Most Important Regulators*, N.Y. TIMES (May 16, 2018) [hereinafter Satariano, *New Privacy*], https://www.nytimes.com/2018/05/16/technology/gdpr-helen-dixon.htmlhttps://www.nytimes.com/2018/05/16/technology/gdpr-helen-dixon.html (Airbnb and Apple likewise have their EU headquarters in Ireland); *see* Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. TIMES (Apr. 27, 2020 [hereinafter Satariano, *Europe's Privacy*], last updated Apr. 28, 2020), https://nyti.ms/2S79ZW8 (Luxembourg's DPA has the responsibility for regulating Amazon).

[418] *See* Satariano*, Europe's Privacy, supra* note 417 (Although Ireland has an "outsize influence" in GDPR enforcement, because of the U.S. Tech Giants that it regulates, its DPA's budget is only sixth among EU DPAs, and it has only been able to obtain a third of the budget increase it sought. However, it has increased staff from 27 in 2017 to 140); *see also* Will Goodbody, *Data Protection Commissioner Defends Speed of Investigations into Tech Firms*, RTE (Jul. 14, 2020, 16:53),

enforcing the GDPR, although assuredly other factors such as low corporate income tax rates, an English speaking population and a business-friendly and common law-based environment have played a role in the decision.[419] However, it may be argued that data subjects benefit from the possibility of forum shopping, as well, as they may choose to file a complaint against a private sector entity with the DPA of either the EU Member State of their "habitual place of residence, place of work, or place of the infringement."[420] The OSS mechanism may not apply in such a case if there is no cross-border processing.[421]

---

https://www.rte.ie/news/technology/2020/0714/1153293-data-protection-commission/ (The head of Ireland's DPA, when asked "whether her office has sufficient resources to regulate tech companies as lead regulator in the EU, she said it depends on how quickly people anticipate outputs will be generated," and elaborate that the authority has, "enough resources and the right resources to conclude, but we can't do it all simultaneously and immediately."); *but see* John Naughton, *Data Protection Laws are Great. Shame They are not Being Enforced*, GUARDIAN (May 2, 2020) (In this opinion piece, the author refers to an investigation by the developers of the Brave browser, and comments that the "most worrying deficit" of technical experts "is in the Irish DPA, which, according to the Brave report, has only 21 tech-enforcement roles. The fact that most of the tech giants have their European HQs in Dublin means that the Irish authority has the heaviest enforcement workload; it's currently the lead authority for 127 cases and yet its budget is being squeezed by the Irish government.").

[419] *See* Vinocur, *supra* note 217 (Ireland is reported to have a "history of law oversight of the technology industry."); *see also* Satariano, *New Privacy*, *supra* note 417.

[420] GDPR, *supra* note 1, art. 77(1); *see e.g.*, Joshua Blume, *A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR*, 49 GEO. J. INT'L L. 1425, 1444 (2018) ("Connected with the "'one stop shop'" provision . . . this will essentially provide data subjects the opportunity to forum shop, finding the DPA with the most bandwidth, availability, and aggressive stance.").

[421] *See* Case C-230/14, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 2015 E.C.L. I-639(Oct. 1, 2015) (In the same vein, but under the EU DP Directive, *Weltimmo* is instructive in that, "Article 4(1)(a) of Directive 95/46 must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out." *Id*. at ¶ 41), http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1159155

One case deserves special attention here: *Google LLC*. In it, the French DPA—the CNIL–received complaints by NOYB and LQDN against Google LLC. On January 21, 2019, the CNIL issued its highest administrative fine ever—for €50 million—against Google LLC in the case for failure to comply with GDPR obligations of transparency and information, and for lack of a legitimate basis for advertising personalization processing.[422] Regarding the OSS mechanism, the CNIL stated the following:

> In this case, the discussions with the other authorities, in particular with the Irish DPA, where GOOGLE's European headquarters are situated, did not allow to consider that GOOGLE had a main establishment in the European Union. Indeed, when the CNIL initiated proceedings, the Irish establishment did not have a decision-making power on the processing operations carried out in the context of the operating system Android and the services provided by GOOGLE LLC, in relation to the creation of an account during the configuration of a mobile phone.
>
> As the "one-stop-shop mechanism" was not applicable, the CNIL was competent to take any decision regarding processing operations carried out by GOOGLE LLC, as were the other DPA.[423]

The CNIL's analysis refers to the concept of "main establishment" discussed in Part II.C.2. Google LLC argued that the CNIL did not have competence to deal with the complaints, as it considered that Google Ireland Limited, its Irish subsidiary, "must be considered its main

---

4; *see also* Waltraut Kotschy, *Article 77 Right to Lodge a Complaint with a Supervisory Authority*, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1117, 1122–23 (Christopher Kuner et al., 2020) (providing a short discussion of the Weltimmo case: a Slovakia registered company targeted exclusively clients in Hungary for its processing activities, and the CJEU considered that the Hungarian DPA could hear claims against the Slovakian company, brought by Hungarian data subjects). When juxtaposed to here, there was no cross-border processing, in the sense of the term's definition set out in Part II.C.2, as only Hungary was concerned by the processing.

[422] *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[423] *Id*.

establishment within the European Union for some of the cross-border processing that it carried out, and particularly that subject of the complaints received by the CNIL."[424] The CNIL considered that in order to be considered the main establishment, Google Ireland Limited would have to "have decision-making power with regard to the processing of the personal data in question."[425]

The CNIL found that the Irish subsidiary was not mentioned in the relevant privacy policy, and that in any event, when the proceedings were initiated there was no proof that Google Ireland Limited possessed decision-making power regarding the relevant processing and that Google LLC was the only developer of the Android operating system involved.[426] Furthermore, Google LLC wrote in a letter to the CNIL "that the "transfer of responsibility" from Google LLC to Google Ireland Limited for certain personal data processing operations relating to European citizens would be complete on January 31, 2019," and the relevant privacy policy would come into effect on January 22, 2019—a day after the CNIL's sanction was issued.[427] As a result, the CNIL considered that Google Ireland Limited was not the main establishment for the processing in question, which allowed the CNIL to act against Google LLC,[428] as the Irish DPA was not then lead DPA. On appeal by Google to France's highest administrative court, the Council of State (*Conseil d'Etat*) agreed with the CNIL that at the time of the decision Google Ireland Limited did not fulfil the criteria to be considered the main establishment for the relevant processing, and thus that there was not then a lead DPA,[429] and rejected Google LLC's petition for the quashing of the sanction.[430]

This case highlights the importance of understanding the law, including all important definitions (such as that of "main establishment"), in assessing the compliance environment, thus looping back to the discussion in Section 2 above. However, it also underscores the ways in which the GDPR helps avoid the use of forum shopping, and focuses on the facts to determine the reality of the data

---

[424] *See* Deliberation No. SAN-2019-001 of the Restricted Committee of the CNIL, *supra* note 114, at 4 (¶ 23).
[425] *Id*. at 5 (¶ 30).
[426] *Id*. at 6 (¶¶ 36–38).
[427] *Id*. at 6 (¶ 39).
[428] *Id*. at 6 (¶ 40–41).
[429] CE, June 19, 2020 (Société Google LLC No. 430810), at 5 (¶ 6), https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil (page and paragraph numbers refer to the PDF form of this decision, downloadable at this address).
[430] *Id*. at 12 (¶ 28).

processing situation on which to base procedural requirements (such as the OSS) intended to help ensure enforcement and, as a result, compliance. This is crystal clear from the text of the Article 29 Working Party Guidelines:

> The GDPR does not permit 'forum shopping'. If a company claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision making over the processing of personal data takes place there, the relevant supervisory authorities (or ultimately EDPB) will decide which supervisory authority is the 'lead', using objective criteria and looking at the evidence.[431]

Thus, in terms of legal strategy, it would seem that efforts at complying with the law, instead of those attempting to avoid compliance through forum shopping, would be more productively spent.

3. Compliance, Non-Compliance and Sanctions

Bagley remarks that in order to realize benefits from corporate resources, legal measures must be implemented by firms; the failure to do so can have "very negative monetary return,"[432] which might be the case if large administrative fines were imposed under the GDPR. Furthermore, shareholder value may be destroyed as a result of violations,[433] and in the area of data privacy, this might be the case if violations lead to loss of customer trust.[434] In contrast, Voss and Houser

---

[431] WP 244, *supra* note 317, at 8.

[432] *See* Bagley, *supra* note 396, at 607–08.

[433] *Id*. at 608.

[434] *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities. The U.S. Department of Commerce has indicated that the lack of trust in Internet privacy in the U.S. is hampering economic activity. *Id.* These privacy concerns continued in a more recent version of the survey. *See* Rafi Goldberg, *Most AMS. Continue to Have Privacy and Security Concerns, NTIA Survey Finds*, NAT'L TELECOMM. & INFO. ADMIN. (Aug. 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds. Voss and Houser point to a decline of Facebook's social media market share as a result of concern regarding loss of privacy and potential security issues, following the Cambridge Analytica scandal. *See* Voss & Houser, *supra* note 22, at 337. That boils down to a loss of trust, which could cause users to be reluctant to share their personal data. *Id*. at 338.

argue that U.S. Tech Giants can use their GDPR compliance to garner trust from their customers.[435] Indeed, the Commission has echoed this view, citing consumer demand for privacy:

> A growing number of companies have responded to this demand for privacy notably by voluntarily extending some of the rights and safeguards provided for in the GDPR to their non-EU based customers. Many businesses also promote respect for personal data as a competitive differentiator and a selling point on the global marketplace, by offering innovative products and services with novel privacy or data security solutions.[436]

Bradford relates that, as companies have failed in lobbying efforts to stop the European Union from regulating through the GDPR, their response may be the "if you cannot beat them, join them" type, lobbying home governments for "EU-equivalent regulation at home."[437] Embracing the GDPR through company compliance efforts may be a way to prepare for any such eventuality, such as GDPR-inspired U.S. State-level legislation.[438]

The GDPR provides incentives for compliance, in the form of factors to be taken into account by DPAs in issuing administrative

---

[435] *See* Voss & Houser, *supra* note 22, at 338.

[436] *See Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizen's Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*, at 3, COM (2020) 264 final (June 24, 2020).

[437] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 256 (2020) (Bradford ties this position to the levelling-the-playing-field argument discussed in Section 1 above: "Given that these firms already have to bear the costs of complying with EU rules, they now have the incentive to advocate further externalization of the single market to their home markets: a strategy that allows them to level the playing field with respect to their domestic, non-export-oriented competitors which, absent domestic regulation, remain unaffected by EU regulations." *Id*.).

[438] *See* Voss & Houser, *supra* note 22, at 340–41 (For example, this action might be true with respect to the California Consumer Privacy Act, as it may also help create efficiencies within firms by applying a high data protection standard worldwide); *see* Voss, *supra* note 395, at 500–01 (Washington State, among other jurisdictions, has also proposed legislation inspired by the GDPR).

fines, somewhat reminiscent of U.S. Sentencing Guidelines.[439] Supervisory authorities are to weigh various factors in deciding whether to impose administrative fines or not, and at which level.[440] These factors include the "nature, gravity and duration of the infringement,"[441] "the intentional or negligent character of the infringement,"[442] whether the controller or processor had previous infringements,[443] and the categories of data infringed,[444] among others. However, other factors allow for the controller or processor to take action in order to improve its position when potential administrative fines are considered or their amount set: for example, action taken by it to mitigate data subject damage,[445] cooperation with the DPAs to remedy the infringement or to mitigate,[446] the fact that the controller or processor notifies the infringement to the DPA itself,[447] or adherence to an approved code of conduct or certification mechanism.[448] Thus, through its understanding of the GDPR, and through adapting its organization and processes to take such measures, a company may seize the opportunity to improve its situation in the unfortunate case of an infringement.

Certain companies may see compliance choices through the prism of risk.[449] They may model this risk based on various factors, such as "formal penalties, reputational impacts on customers, organizational morale costs, relations with regulators, and perceptions of society."[450] In the context of the GDPR, given its short period of application to date, there is a chance that any such model would be skewed, given the implementation time that has been needed prior to jurisdictions such as Ireland being ready to assess major administrative fines. That is, the "formal penalties" factor would potentially be understated and reduce the modelized consequences of non-compliance. If we imagine that firms engage in a tradeoff between

---

[439] *See* Voss, *supra* note 16, at 818–19.
[440] GDPR, *supra* note 1, art. 83(2).
[441] *Id*. art. 83(2)(a).
[442] *Id*. art. 83(2)(b).
[443] *Id*. art. 83(2)(e).
[444] *Id*. art. 83(2)(g).
[445] GDPR, *supra* note 1, art. 83(2)(c).
[446] *Id*. art. 83(2)(f).
[447] *Id*. art. 83(2)(h).
[448] *Id*. art. 83(2)(j).
[449] *See* Bird & Park, *supra* note 408, at 297.
[450] *Id*. at 299.

expending resources for compliance or, alternatively, accepting to pay sanctions,[451] their analysis would potentially be erroneous.

Indeed, there have been signs that companies—and first among them, the U.S. Tech Giants—should expect significant administrative sanctions in the future. First, the head of the Irish DPA—Helen Dixon, the Data Protection Commissioner—has sounded the alarm that concluding major investigations into what are surely the U.S. Tech Giants, is the Irish DPA's top priority.[452] Earlier in the year, she is reported to have said that "rulings involving Twitter, Facebook and others were coming."[453] In 2019, she commented that fines will be "substantial."[454] Just before the application date for the GDPR, Dixon said, in answer to a question on whether she had a message for Facebook CEO Mark Zuckerberg and other tech executives, "they should expect her to use her new powers to "to the fullest."[455]

Dixon put the risk of sanctions in terms that a compliance officer can understand, referring at the start to the one-off fine that FTC had previously announced against Facebook:

> "While big figures have been bandied about in terms of a one-off settlement, the GDPR is going to be with us probably for another 20 years," said Dixon. "And in each of the investigations, fines can be applied in each separate case."
>
> "As new issues keep arising, we'll keep investigating and pursuing," she said. "So in a very theoretical sense, if we're forced based on a risk-based

---

[451] *Id*. at 301 ("The choice to either invest in compliance or pay the cost of non-compliance implies imperfect substitutes. Firms can switch between compliance and sanction, but the tradeoff is not identical.").

[452] *See* Goodbody, *supra* note 418 ("The Data Protection Commissioner has said concluding investigations that are underway into large multinational tech firms is the number one priority for her office," and has previously mentioned investigations into Facebook, WhatsApp, Instagram and Twitter).

[453] *Privacy Advocates' Complaints Overwhelm Data Protection Office*, IRISH TIMES (Apr. 28, 2020, 16:49), https://www.irishtimes.com/business/technology/privacy-advocates-complaints-overwhelm-data-protection-office-1.4240175.

[454] Angelique Carson, *Dixon at Senate Hearing: Fines are Coming; They Will be 'Substantial'*, IAPP (May 2, 2019), https://iapp.org/news/a/dixon-at-senate-hearing-fines-are-coming-they-will-be-substantial/.

[455] Satariano, *New Privacy*, *supra* note 417.

> analysis to keep opening investigations, the fines are going to mount up over time."[456]

Furthermore, mounting pressure is being placed on Ireland to act[457] from many sources, such as EU government leaders,[458] privacy advocates[459] and other DPAs.[460] Nonetheless, the Irish DPA is reported to have provided a draft decision on an investigation of Twitter to other EU DPAs under the OSS mechanism.[461] Moreover, given the results of

---

[456] Nancy Scola, *Irish Data Official Defends Tech Investigation Record: 'They're not Overnight'*, POLITICO (May 4, 2019, 9:57 AM CET, updated May 6, 2019, 3:13 PM CET), https://www.politico.eu/article/helen-dixon-irish-data-official-defends-tech-investigation-record-theyre-not-overnight/.

[457] *See*, *e.g.*, Mark Scott, *EU Privacy Enforcer Hits Make-or-Break Moment*, POLITICO (May 21, 2020, 6:00 AM CET), https://www.politico.com/news/2020/05/21/europe-data-protection-agency-ireland-272889 ("With the two-year anniversary of Europe's privacy standards coming next Monday, Dixon is under mounting pressure to show that her agency can act.").

[458] *See* Satariano*, Europe's Privacy*, *supra* note 417 ("The inaction is creating tensions within European governments, as some leaders call for speedier enforcement and broader changes.").

[459] *See Open Letter: EDRi Urges Enforcement and Actions for the 2 Year Anniversary of the GDPR*, EDRI (May 25, 2020), https://edri.org/open-letter-edri-urges-enforcement-and-actions-for-the-2-year-anniversary-of-the-gdpr/ (the user digital rights organization, without naming Ireland specifically, wrote to the Commission to "urge action to tackle the GDPR's vast enforcement gap."); *see also* NOYB - European Center for Digital Rights, *NOYB Letter to the European Data Protection Authorities, the European Data Protection Board, the European Commission and the European Parliament* (May 25, 2020), https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf ("The GDPR is only as strong as its weakest DPA: In practice, this is perhaps best illustrated by the fact that the Irish DPC has so far not issued a single fine under the GDPR against a private actor, despite reporting 7,215 complaints in 2019 and staff of more than 130. It comes as no surprise that Google immediately tried to switch to the jurisdiction of the Irish DPC right after the French CNIL issued its fine in the parallel procedure cited above.").

[460] *See* Scott, *supra* note 457 (describing some EU regulators as considering that Ireland is "dragging its feet." "'You don't hear anything about cases transferred to Ireland,' says Johannes Caspar, head of Hamburg's data protection regulator, whose agency is the first port of call for privacy complaints about almost all U.S. tech firms in Germany. 'What goes on, what types of information was exchanged, we don't get any of that. We're here just standing and waiting.'").

[461] Natasha Lomas, *First Major GDPR Decisions Looming on Twitter and Facebook*, TECHCRUNCH (May 22, 2020, 9:30 PM CEST),

the Commission's two-year GDPR evaluation detailed in part II.D., greater cooperation between DPAs and additional funding for DPAs such as the Irish DPA should be forthcoming, which should help further enforcement and lead to larger fines of the U.S. Tech Giants that violate the GDPR, as provided for in the GDPR, unless they categorically abandon the European market, which is unrealistic. In this context, the GDPR's cooperation and consistency mechanism should be of great use.

B. Risks Involved with GDPR Non-Enforcement

As Wojciech Rafał Wiewiórowski—the European Data Protection Supervisor—recently stated, "Effective enforcement is an important element of any data protection framework."[462] An evaluation of the effectiveness of GDPR enforcement to-date is relevant to this study, and the institutional evaluation of the GDPR has been detailed in Part II.D.

DPA communications are important as indicating what action the regulator intends to take, thus providing companies with information that will help shape their compliance programs. Interestingly, DPAs have tended to minimize the role of sanctions or, alternatively, to highlight the policy goals for their use, while many companies have been focused on the issue. For example, the ICO addressed the issue of GDPR sanctions early on in a "myth-busting" blog post.[463] Information Commissioner Elizabeth Denham said that the GDPR "is not about fines," adding that it is "about putting the consumer and the citizen first."[464] She emphasized the educational role played by the DPA, and the importance of other enforcement tools which have an impact on reputation:

> … it's scaremongering to suggest that we'll be making early examples of organisations for minor

https://techcrunch.com/2020/05/22/first-major-gdpr-decisions-looming-on-twitter-and-facebook/.

[462] European Data Protection Supervisor, *The EDPS Strategy 2020 – 2024: Shaping a Safer Digital Future* (2020), https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf.

[463] Elizabeth Denham, *GDPR – Sorting the Fact from the Fiction*, ICO BLOG (Aug. 9, 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/blog-gdpr-sorting-the-fact-from-the-fiction/ ("Myth #1: The biggest threat to organisations from the GDPR is massive fines.").

[464] *Id*.

> infringements or that maximum fines will become the norm.
>
> The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick.
>
> … we have yet to invoke our maximum powers.
>
> Predictions of massive fines under the GDPR that simply scale up penalties we've issued under the Data Protection Act are nonsense.
>
> Don't get me wrong, the UK fought for increased powers when the GDPR was being drawn up. Heavy fines for serious breaches reflect just how important personal data is in a 21st century world.
>
> But we intend to use those powers proportionately and judiciously.
>
> And while fines may be sledgehammer in our toolbox, we have access to other tools that are well-suited to the task at hand and just as effective.
>
> Like the DPA, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow.
>
> And you can't insure against that.[465]

These comments are very interesting and illustrate the philosophy that some regulators may develop, namely that the administrative sanctions provided for in the GDPR mainly have an expressive function. From this perspective, the symbolic function does not require effective impositions of sanctions.[466]

Moreover, a discourse like that of the UK DPA emphasizes that the attitude of DPAs towards sanctions is definitely that of a regulator, and not that of a criminal judge whose job it is basically to pronounce sentences if offenses are proven, as soon as the repressive rule is

---

[465] *Id*.

[466] *See supra* Part I. C.

operative.[467] In the case of regulators, it appears clearly that sanctions are merely a means of fulfilling their role and enforcing the legal framework set up by the lawmaker.[468] In the initial phase, when the GDPR had to be applied by businesses, the regulators' discourse was that priority was given to education and support for actors to help them to put in place solutions to comply with the new regulation.[469] Without affirming that sanctions would not be imposed, the message was that companies, especially SMEs, should not be overly afraid of sanctions and that they should instead engage in a cooperative approach with the regulator. Thus, there was a kind of two-fold caveat about sanctions: (i) sanctions would not be the first response to difficulties in immediately applying the new regulations; and (ii) the regulation would differentiate between large firms and smaller firms with less expertise to implement the GDPR. The interpretation to be given to the position of regulators should therefore take into account that the initial, "educational" phase may be over and that these reassuring words about the risk of sanctions may not apply to tech giants. A third points should be mentioned: Information Commissioner Denham's words express the opinion of a person responsible for a particular DPA, especially one from a country that is no longer a member of the European Union, with the end of the Brexit transition period soon

---

[467] Daniel Ohana, *Regulatory Offenses and Administrative Sanctions: Between Criminal and Administrative Law*, The Oxford Handbook of Criminal Law, (M. D. Dubber & T. Hörnle, 2014).

[468] Achour M. Taibi Achour, *La justification du pouvoir de sanction des AAI de régulation est-elle toujours pertinente?* [Is the Justification for the Sanctioning Power of Regulatory IAAs Still Relevant?], 84 REVUE INTERNATIONALE DE DROIT PÉNAL 463, 463 (2013).

[469] *See* Catherine Stupp, *Falque-Pierrotin Leaves Top EU Post Before Dawn of 'New Era' for Privacy*, EURACTIV (Feb. 8, 2018), https://www.euractiv.com/section/data-protection/interview/falque-pierrotin-leaves-top-eu-post-before-dawn-of-new-era-for-privacy/ (quoting Isabelle Falque-Pierrotin, then outgoing head of the Article 29 Data Protection Working and head of the CNIL about then-forthcoming application of the GDPR, "It means the national authorities have to invest also in regulatory dialogue with the actors to provide them with a compliance tool that is very flexible, deciding the provision of the regulation in a more operational way. We've started this sectoral conversation with the actors in France and I believe in most of the countries we're going to have this type of demand from stakeholders. Because of course they want to avoid fines, it's normal. It's our job as regulators to help them comply. Our job is not to have fines at any price.").

ahead on December 31, 2020.[470] It cannot be excluded that divergences between the policies pursued by the different national DPAs will increase during the current period. The DPAs might have different ideas on whether the initial pedagogical phase is over and whether it is not appropriate to have strong expectations vis-à-vis the tech giants.[471] These advanced or dissenting assessments could lead some DPAs to consider applying sanctions against tech giants, as the French CNIL has started to do against Google, or even to consider applying severe sanctions, as it is not yet the case.

While such measures may have many goals, including perhaps some political ones, they should be modelled in a way that does not undercut the theoretical goals of the GDPR's sanctions, including notably the deterrence function discussed in Part I.D. Furthermore, the lack of heavy sanctions and of effective enforcement by the Irish DPA to date poses a difficulty in light of the theory of sanctions. Particularly, to date sanctions have not been significantly large so as to sufficiently encourage the U.S. Tech Giants to comply with the GDPR. Furthermore, effective sanctioning is needed for the symbolic function, to send a message to market participants. This has been lacking in Ireland up to present. Finally, as this study discussed in Section III.A., companies do analyze past sanctions through modeling to evaluate risk of non-compliance. Thus, there is a danger that a lack of large, effective sanctions, may be giving a signal that the U.S. Tech Giants may continue to consider the risk of GDPR sanctions as a mere cost of doing business.

IV. RECOMMENDATIONS

Two and one-half years after Axelle Lemaire made her comment about sanctions, and two months after the GDPR entered into application, Facebook's shares lost about from twenty percent to a quarter of their value, attributed in part to expected costs of the privacy-enhancing requirements of the GDPR and also to loss of users due to scandals such as the Cambridge Analytica case involving misuse of

[470] UK Prime Minister Boris Johnson is reported to have indicated that the UK would diverge from the European Union on data protection law when the blocs split. There is also no guarantee that the UK will receive an adequacy decision for cross-border data transfers. *See* Jorge Valero & Samuel Stolton, *LEAK: Commission Pushes UK for 'High Degree of Convergence' in GDPR Review*, EURACTIV (June 23, 2020, updated June 24, 2020), https://www.euractiv.com/section/digital/news/leak-commission-pushes-uk-for-high-degree-of-convergence-in-gdpr-review/ (If no agreement is reached on an adequacy decision, controllers will not be able to export personal data from the European Union to the UK without additional safeguards.).

[471] *See* Golla, *supra* note 67, at 72–73.

personal data.[472] In the market value ranking of the U.S. Tech Giants, the two companies arguably the most dependent on the use of personal data for advertising—Google and Facebook—both slipped between 2017 and 2019. Alphabet (Google) went from second to fourth place and Facebook from fourth to fifth.[473] This article argues that Lemaire's comment and the news are related—that the fact of having higher sanctions—if effectively applied—should give Facebook (and other data-consuming companies) the incentive it needs to comply with EU data protection law, and that, although compliance may involve costs, it in turn may result in benefits to firms (such as the avoidance of sanctions and related legal costs and staff time, or eventually increased trust in the eyes of the consumer and thus advanced compliance with personal data law may ultimately appear to be a competitive advantage in the market compared to other less scrupulous companies.)[474] and further, that previously the lack of adequate sanctions gave companies such as Facebook no effective incentive originating in law to truly guarantee user data protection. Effective and substantial fines should result in the deterrence effect, which perhaps does not yet exist because of the failure to date of the Irish DPA to bring to completion enforcement action against the U.S. Tech Giants.

Also, DPAs must pay more attention to the message that they communicate. While DPAs such as the United Kingdom's ICO might be eager to reassure stakeholders that "Predictions of massive fines . . . are nonsense," as Commissioner Denham was quoted as saying in Part III.B., they should consider the impact that this has on the deterrent effect of those same sanctions, especially on the U.S. Tech Giants and similar companies in China, India, and elsewhere. While such measures may have many goals, including perhaps some political ones, they should be modelled in a way that does not undercut the theoretical

---

[472] *See* Vengattil Munsif & Dave Paresh, *Facebook's Grim Forecast: Privacy Push Will Erode Profits for Years*, REUTERS (July 25, 2018, 10:11 PM), https://www.reuters.com/article/us-facebook-results/facebooks-grim-forecast-privacy-push-will-erode-profits-for-years-idUSKBN1KF2U5. *See also*, Hannah Kuchler, *Facebook Shares Take a Hit After Poor Results*, FIN. TIMES (July 25, 2018), https://www.ft.com/content/c0097b18-9028-11e8-bb8f-a6a2f7bca546.

[473] S*ee* Kenneth Kiesnoski, *The Top 10 US Companies by Market Capitalization*, CNBC (Mar. 8, 2017, 7:53 AM EST, updated Oct. 24, 2017, 2:22 PM EDT), https://www.cnbc.com/2017/03/08/the-top-10-us-companies-by-market-capitalization.html (For the ranking as of October 24, 2017).

[474] *See* Voss & Houser, *supra* note 22, at 334–40 (Arguing that compliance with provisions of the GDPR, even beyond what is necessary, for example by extending GDPR-like protections to consumers worldwide, may constitute an element of legal strategy).

goals of the GDPR's sanctions, including notably the deterrence function discussed in Part I.D. The other conclusion that can be drawn from the preceding remarks is that it would be important that the different policies of the DPAs regarding the use of sanctions be harmonized, both for the legal certainty in favor of businesses and for the credibility of the regulatory policy.

Nonetheless, as a result of this potential for greatly reinforced enforcement measures and sanctions in the near future, companies (especially the U.S. Tech Giants) must ensure that their risk assessment tools are not too grounded in the past, and adequately take count of probable future changes. They should consider that big sanctions—those that deter violations and demand compliance—are presumably on their way in Ireland and perhaps elsewhere.

In their discussion of GDPR compliance,[475] Voss and Houser refer to a legal strategy theoretical framework of compliance pathways developed by Bird.[476] Five stages are detailed in that framework: avoidance, compliance, prevention, advantage, and transformation, ordered with respect to the degree of business transformation, with the highest degree at the end (transformation).[477] Indeed, compliance with regulation not only may reward companies with trust but may bring other benefits, which argues in favor of companies' embracing compliance. As an example, by making efforts to comply with the GDPR, companies will be preparing themselves for future changes to laws of countries that will be impacted by the GDPR, through negotiations between them and the European Union leading to adequacy decisions. Thus, embracing the GDPR now will prepare them for the future in other jurisdictions, including U.S. states whose legislation is inspired by the GDPR.[478] Furthermore, even new economic actors may pop up, seizing an opportunity, such as those of the privacy tech sector.[479]

Looking forward, the reader could imagine an extreme case of the risk of sanctions (for example the maximum incurred) applied to one of the U.S. Tech Giants, motivated by an anti-U.S. Tech Giants us-versus-them spirit. A national DPA such as the CNIL could react

---

[475] *Id.* at 329–40.

[476] Robert C. Bird, *Pathways of Legal Strategy*, 14 STAN. J.L. BUS. & FIN. 1 (2008).

[477] *Id*. at 11.

[478] *See* Voss & Houser, *supra* note 22, at 335–36 (For a discussion of this in the case of Microsoft's extension of GDPR rights to its other customers); *see* Voss, *supra* note 395, 516–17 (Regarding the extension of EU data privacy standards through adequacy decision negotiations).

[479] *See*, *e.g.*, Tene, *supra* note 13 (citing as examples OneTrust, TrustArc, Privitar, BigID and WireWheel).

vigorously against a clear or even scandalous violation of the rights of Internet users (think of the Cambridge Analytica affair) and seek to "mark the spirits" by imposing an exemplary sanction. The impact would not only be financial for the sanctioned company; it would also be competitive. The digital services offered by the tech giants are partly specific and partly common to the different companies. For example, Google is dominant on the market for search engines,[480] Facebook is dominant on the market for social networks, and so on.[481] However, the various giants are in competition with each other in part of their business, particularly in the advertising exploitation of site traffic from the platforms that these companies offer.[482] Each company, therefore, runs the risk of being threatened by a regulatory decision that would weaken it and affect user confidence vis-à-vis it. If one of the dominant companies in the digital economy commits serious violations of the GDPR and is therefore heavily sanctioned (through a heavy fine and a compliance order), then that company risks being seriously harmed. The exploitation of personal data is at the heart of their business model. If it is the way it collects, processes, and trades data that is considered to be contrary to the GDPR, then its business model needs to be thoroughly revised.[483] Such a challenge would certainly be costly and time-consuming to implement. In the meantime, there is a risk that competing firms may gain a lead that the sanctioned firm may have difficulty catching up to. The history of the digital economy, and of technology firms more generally, has shown that apparent dominance at one point in time does not prevent rapid relegation.[484] Thus, the challenge for each tech giants is not only to be sufficiently compliant

---

[480] *See* Simon van Dorpe & Leah Nylen, *Europe Failed to Tame Google. Can the US do Any Better?*, POLITICO (Oct. 22, 2020, 6:30 AM), https://www.politico.eu/article/europe-failed-to-tame-google-can-the-us-do-any-better/.

[481] *See* Cecilia Kang, *F.T.C. Decision on Pursuing Facebook Antitrust Case Is Said to Be Near*, N.Y. TIMES (Oct. 22, 2020), https://nyti.ms/3jqJs0O.

[482] *See* Rodrigo Salvaterra, *Who is Winning: Google, Amazon, Facebook, or Apple?,* TOWARDS DATA SCIENCE (Feb. 10, 2020), https://towardsdatascience.com/who-is-winning-google-amazon-facebook-or-apple-45728660473.

[483] Bertin Martens, JRC TECHNICAL REPORTS, AN ECONOMIC POLICY PERSPECTIVE ON ONLINE PLATFORMS 39–46 (Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05 JRC101501), (2016) (*See* https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf).

[484] *See*, *e.g.*, Walter Frick, *The Decline of Yahoo in Its Own Words*, HARV. BUS. REV. (June 2, 2016), https://hbr.org/2016/06/the-decline-of-yahoo-in-its-own-words.

with the GDPR in order not to be exposed to sanctions, but also not to be less compliant than other major market players so as not to risk that a possible sanction becomes a serious competitive disadvantage. While this scenario remains hypothetical, it is a possibility that leads us to recommend taking the risk of sanctions by the DPAs seriously.

CONCLUSION

Prior to the application of the GDPR, on May 25, 2018, one of the results of the relatively-low-level of legislatively permitted data protection violation administrative fines was, arguably, a lack of compliance by U.S. Tech Giants, among others. At least on paper, this changed under the GDPR. This study has approached the issue of GDPR sanctions, not through the lens of a future catastrophe, but through, first developing the theoretical grounds for sanctions, prior to viewing the practical side of them. In doing so, it has been somewhat unique and has added to the GDPR literature. Furthermore, it has engaged the legal strategy and compliance literature to bring its results home to inform companies as to the risks involved and to provide strategic recommendations.

Of the several sub-goals of sanctions, this study has determined that the most relevant for an analysis of GDPR sanctions—which are administrative, regulatory, and financial sanctions, in large part—is the deterrence function, beyond the symbolic functions. This demands effective and substantial administrative fines. While these are not the only sanctions available under the GDPR—this study has also set out a range of possible sanctions, such as judicial compensation and orders to halt data processing—they are perhaps the most characteristic of data protection enforcement. However, through what is referred to as the OSS mechanism, the Irish DPA is the lead authority for most of the U.S. Tech Giants, and it has failed to act against them up to now, resulting in a potential lack of deterrence.

This study argues that companies should not take this recent past as a sign of the future, and should assume that bigger fines are coming, including those that should be issued by Ireland's DPA. This is because Ireland has been hampered by problems of limited resources but should be on the verge of a decision on Twitter, and the finalizing of investigations against other U.S. Tech Giants. Pressure coming from various sources (public opinion, peer DPAs, etc.) is being put on the Irish DPA to do exactly this, and the OSS and cooperation and consistency mechanisms under the GDPR should help. Furthermore, the Commission is pushing Member States to provide greater resources to DPAs, and the EDPB to work on greater cooperation among DPAs. Thus, companies should seize the reputational and other benefits of

GDPR compliance, and not base compliance risk modeling on the sanctions that have been issued during what has turned out to be the GDPR's breaking-in period.

At the same time, DPAs (and the EDPB) must be aware of the importance of enforcement action. Truly dissuasive administrative fines must be issued in order for the sanctions to have their necessary deterrence effect. Furthermore, as has been shown, companies watch the past to predict the future, so it is important to signal to them that compliance is being taken very seriously.